Audit Report

Audit Report Sample

Audited on June 24, 2015

Reported on June 24, 2015

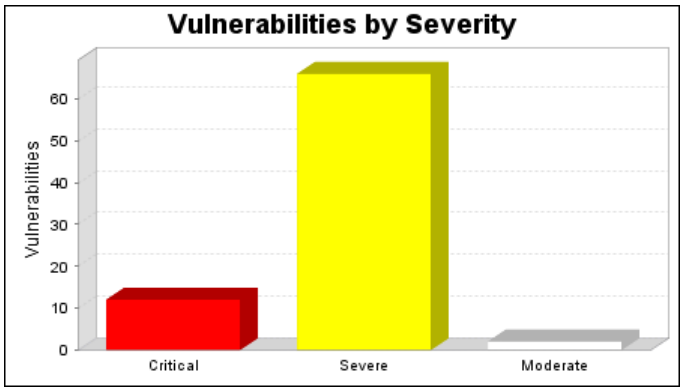
1. Executive Summary

This report represents a security audit performed by Nexpose from Rapid7 LLC. It contains confidential information about the state of your network. Access to this information by unauthorized personnel may allow them to compromise your network.

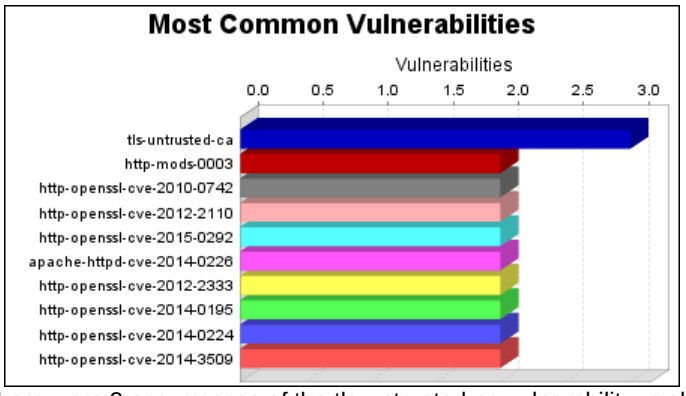
Site Name	Start Time	End Time	Total Time	Status
http://xx.xxx.xx.xxx	June 24, 2015 16:32, AEST	June 24, 2015 16:41, AEST	9 minutes	Success

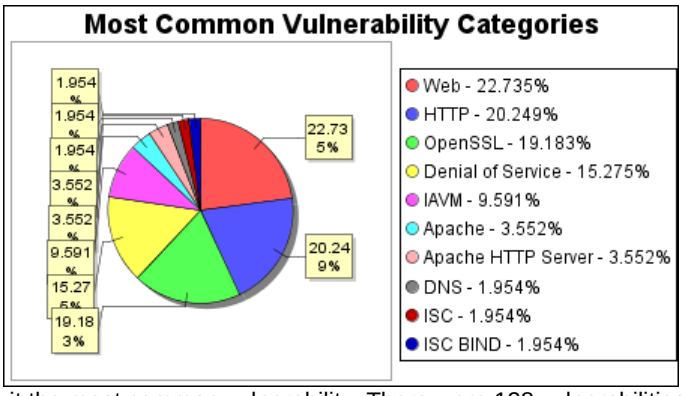
There is not enough historical data to display overall asset trend.

The audit was performed on one system which was found to be active and was scanned.

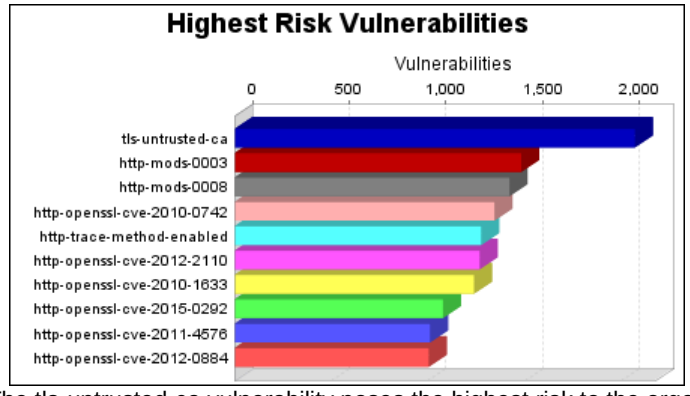


There were 80 vulnerabilities found during this scan. Of these, 12 were critical vulnerabilities. Critical vulnerabilities require immediate attention. They are relatively easy for attackers to exploit and may provide them with full control of the affected systems. 66 vulnerabilities were severe. Severe vulnerabilities are often harder to exploit and may not provide the same access to affected systems. There were 2 moderate vulnerabilities discovered. These often provide information to attackers that may assist them in mounting subsequent attacks on your network. These should also be fixed in a timely manner, but are not as urgent as the other vulnerabilities.





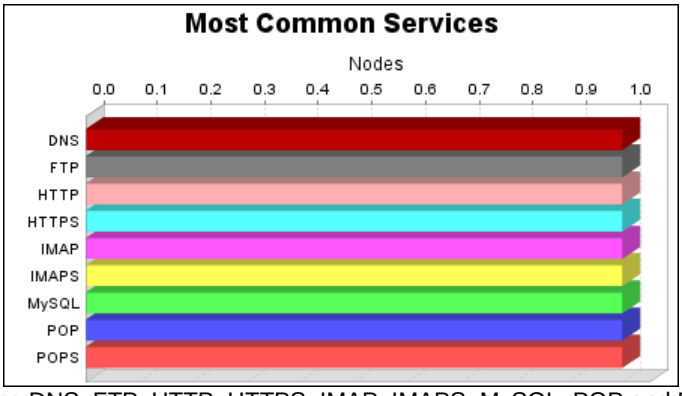
There were 3 occurrences of the tls-untrusted-ca vulnerability, making it the most common vulnerability. There were 128 vulnerabilities in the Web category, making it the most common vulnerability category.

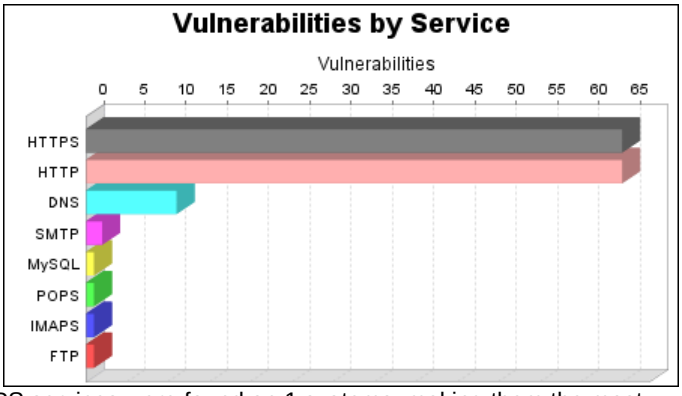


The tls-untrusted-ca vulnerability poses the highest risk to the organization with a risk score of 2,072. Risk scores are based on the

types and numbers of vulnerabilities on affected assets.
One operating system was identified during this scan.

There were 11 services found to be running during this scan.





The DNS, FTP, HTTP, HTTPS, IMAP, IMAPS, MySQL, POP and POPS services were found on 1 systems, making them the most common services. The HTTPS and HTTP services were found to have the most vulnerabilities during this scan, each with 65 vulnerabilities.

2. Discovered Systems

Node	Operating System	Risk	Aliases
xx.xxx.xx.xxx	xxxxxxxx	22,191	• Xx.xxx.xx.xxx Xx.xxx.xx.xxx

3. Discovered and Potential Vulnerabilities

3.1. Critical Vulnerabilities

3.1.1. ISC BIND: Handling of zero length rdata can cause named to terminate unexpectedly (CVE-2012-1667) (dns-bind-cve-2012-1667)

Description:

ISC BIND 9.x before 9.7.6-P1, 9.8.x before 9.8.3-P1, 9.9.x before 9.9.1-P1, and 9.4-ESV and 9.6-ESV before 9.6-ESV-R7-P1 does not properly handle resource records with a zero-length RDATA section, which allows remote DNS servers to cause a denial of service (daemon crash or data corruption) or obtain sensitive information from process memory via a crafted record.

Affected Nodes:

Affected Nodes:	Additional Information:
xx.xxx.xx.xxx:53	• Running DNS service • Product BIND exists -- BIND 9.8.2rc1-RedHat-9.8.2-0.23.rc1.el6_5.1 Vulnerable version of product BIND found -- BIND 9.8.2rc1-RedHat-9.8.2-0.23.rc1.el6_5.1

References:

Source	Reference
APPLE	APPLE-SA-2012-09-19-2
CVE	CVE-2012-1667
DISA_SEVERITY	Category I
DISA_VMSKEY	V0035032
IAVM	2012-A-0189
REDHAT	RHSA-2012:1110
URL	https://kb.isc.org/article/AA-00698/0
URL	https://kb.isc.org/article/AA-00698/74/CVE-2012-1667%3A-Handling-of-zero-length-rdata-can-cause-named-to-terminate-unexpectedly.html

Vulnerability Solution:

More information about upgrading your version of ISC BIND is available on the ISC website.

3.1.2. Obsolete ISC BIND installation (dns-bind-obsolete)

Description:

ISC BIND versions before 9.9 are considered obsolete. ISC will not fix security bugs in these versions (even critical ones).

It is strongly recommended that you upgrade your BIND installation to a supported version.

Affected Nodes:

Affected Nodes:	Additional Information:
xx.xxx.xx.xxx:53	• Running DNS service • Product BIND exists -- BIND 9.8.2rc1-RedHat-9.8.2-0.23.rc1.el6_5.1 Vulnerable version of product BIND found -- BIND 9.8.2rc1-RedHat-9.8.2-0.23.rc1.el6_5.1

References:

Source	Reference
URL	https://kb.isc.org/article/AA-00913/0/BIND-9-Security-Vulnerability-Matrix.html
URL	https://www.isc.org/software/bind

Vulnerability Solution:

More information about upgrading your version of ISC BIND is available on the ISC website.

3.1.3. ISC BIND: Heavy DNSSEC validation load can cause a "bad cache" assertion failure (CVE-2012-3817) (dns-bind-cve-2012-3817)

Description:

ISC BIND 9.4.x, 9.5.x, 9.6.x, and 9.7.x before 9.7.6-P2; 9.8.x before 9.8.3-P2; 9.9.x before 9.9.1-P2; and 9.6-ESV before 9.6-ESV-R7-P2, when DNSSEC validation is enabled, does not properly initialize the failing-query cache, which allows remote attackers to cause a denial of service (assertion failure and daemon exit) by sending many queries.

Affected Nodes:

Affected Nodes:	Additional Information:
xx.xxx.xx.xxx:53	• Running DNS service • Product BIND exists -- BIND 9.8.2rc1-RedHat-9.8.2-0.23.rc1.el6_5.1 Vulnerable version of product BIND found -- BIND 9.8.2rc1-RedHat-9.8.2-0.23.rc1.el6_5.1

References:

Source	Reference
APPLE	APPLE-SA-2013-09-12-1
CVE	CVE-2012-3817
DEBIAN	DSA-2517
DISA_SEVERITY	Category I
DISA_VMSKEY	V0035032
IAVM	2012-A-0189
REDHAT	RHSA-2012:1122
REDHAT	RHSA-2012:1123
URL	https://kb.isc.org/article/AA-00729/0
URL	https://kb.isc.org/article/AA-00729/74/CVE-2012-3817%3A-Heavy-DNSSEC-Validation-Load-Can-Cause-a-Bad-Cache-Assertion-Failure-in-BIND9.html

Vulnerability Solution:

More information about upgrading your version of ISC BIND is available on the ISC website.

3.1.4. ISC BIND: A specially crafted Resource Record could cause named to terminate (CVE-2012-4244) (dns-bind-cve-2012-4244)

Description:

ISC BIND 9.x before 9.7.6-P3, 9.8.x before 9.8.3-P3, 9.9.x before 9.9.1-P3, and 9.4-ESV and 9.6-ESV before 9.6-ESV-R7-P3 allows remote attackers to cause a denial of service (assertion failure and named daemon exit) via a query for a long resource record.

Affected Nodes:

Affected Nodes:	Additional Information:
xx.xxx.xx.xxx:53	• Running DNS service • Product BIND exists -- BIND 9.8.2rc1-RedHat-9.8.2-0.23.rc1.el6_5.1 Vulnerable version of product BIND found -- BIND 9.8.2rc1-RedHat-9.8.2-0.23.rc1.el6_5.1

References:

Source	Reference
APPLE	APPLE-SA-2013-09-12-1
CVE	CVE-2012-4244
DEBIAN	DSA-2547
DISA_SEVERITY	Category I
DISA_VMSKEY	V0036787
IAVM	2013-A-0031
REDHAT	RHSA-2012:1266
REDHAT	RHSA-2012:1267
REDHAT	RHSA-2012:1268
REDHAT	RHSA-2012:1365
URL	https://kb.isc.org/article/AA-00778/0
URL	https://kb.isc.org/article/AA-00778/74/CVE-2012-4244%3A-A-specially-crafted-Resource-Record-could-cause-named-to-terminate.html

Vulnerability Solution:

More information about upgrading your version of ISC BIND is available on the ISC website.

3.1.5. ISC BIND: Specially crafted DNS data can cause a lockup in named (CVE-2012-5166) (dns-bind-cve-2012-5166)

Description:

ISC BIND 9.x before 9.7.6-P4, 9.8.x before 9.8.3-P4, 9.9.x before 9.9.1-P4, and 9.4-ESV and 9.6-ESV before 9.6-ESV-R7-P4 allows remote attackers to cause a denial of service (named daemon hang) via unspecified combinations of resource records.

Affected Nodes:

Affected Nodes:	Additional Information:
xx.xxx.xx.xxx:53	• Running DNS service • Product BIND exists -- BIND 9.8.2rc1-RedHat-9.8.2-0.23.rc1.el6_5.1 Vulnerable version of product BIND found -- BIND 9.8.2rc1-RedHat-9.8.2-0.23.rc1.el6_5.1

References:

Source	Reference
APPLE	APPLE-SA-2013-09-12-1
BID	55852
CVE	CVE-2012-5166
DEBIAN	DSA-2560
OSVDB	86118
OVAL	OVAL19706
REDHAT	RHSA-2012:1363
REDHAT	RHSA-2012:1364
REDHAT	RHSA-2012:1365
URL	https://kb.isc.org/article/AA-00801/0
URL	https://kb.isc.org/article/AA-00801/74/CVE-2012-5166%3A-Specially-crafted-DNS-data-can-cause-a-lockup-in-named.html

Vulnerability Solution:

More information about upgrading your version of ISC BIND is available on the ISC website.

3.1.6. ISC BIND: BIND 9 servers using DNS64 can be crashed by a crafted query (CVE-2012-5688) (dns-bind-cve-2012-5688)

Description:

ISC BIND 9.8.x before 9.8.4-P1 and 9.9.x before 9.9.2-P1, when DNS64 is enabled, allows remote attackers to cause a denial of service (assertion failure and daemon exit) via a crafted query.

Affected Nodes:

Affected Nodes:	Additional Information:
xx.xxx.xx.xxx:53	• Running DNS service • Product BIND exists -- BIND 9.8.2rc1-RedHat-9.8.2-0.23.rc1.el6_5.1 Vulnerable version of product BIND found -- BIND 9.8.2rc1-RedHat-9.8.2-0.23.rc1.el6_5.1

References:

Source	Reference

Source	Reference
APPLE	APPLE-SA-2013-09-12-1
CVE	CVE-2012-5688
REDHAT	RHSA-2012:1549
URL	https://kb.isc.org/article/AA-00828/0
URL	https://kb.isc.org/article/AA-00828/74/CVE-2012-5688%3A-BIND-9-servers-using-DNS64-can-be-crashed-by-a-crafted-query.html

Vulnerability Solution:

More information about upgrading your version of ISC BIND is available on the ISC website.

3.1.7. ISC BIND: A specially crafted query can cause BIND to terminate abnormally (CVE-2013-4854) (dns-bind-cve-2013-4854)

Description:

The RFC 5011 implementation in rdata.c in ISC BIND 9.7.x and 9.8.x before 9.8.5-P2, 9.8.6b1, 9.9.x before 9.9.3-P2, and 9.9.4b1, and DNSco BIND 9.9.3-S1 before 9.9.3-S1-P1 and 9.9.4-S1b1, allows remote attackers to cause a denial of service (assertion failure and named daemon exit) via a query with a malformed RDATA section that is not properly handled during construction of a log message, as exploited in the wild in July 2013.

Affected Nodes:

Affected Nodes:	Additional Information:
xx.xxx.xx.xxx:53	• Running DNS service • Product BIND exists -- BIND 9.8.2rc1-RedHat-9.8.2-0.23.rc1.el6_5.1 Vulnerable version of product BIND found -- BIND 9.8.2rc1-RedHat-9.8.2-0.23.rc1.el6_5.1

References:

Source	Reference
APPLE	APPLE-SA-2014-10-16-3
BID	61479
CVE	CVE-2013-4854
OVAL	OVAL19561
REDHAT	RHSA-2013:1114
REDHAT	RHSA-2013:1115
URL	https://kb.isc.org/article/AA-01015/0
URL	https://kb.isc.org/article/AA-01015/74/CVE-2013-4854%3A-A-specially-crafted-query-can-cause-BIND-to-terminate-abnormally.html
XF	86004

Vulnerability Solution:

More information about upgrading your version of ISC BIND is available on the ISC website.

3.1.8. ISC BIND: A Defect in Delegation Handling Can Be Exploited to Crash BIND (CVE-2014-8500) (dns-bind-cve-2014-8500)

Description:

ISC BIND 9.0.x through 9.8.x, 9.9.0 through 9.9.6, and 9.10.0 through 9.10.1 does not limit delegation chaining, which allows remote attackers to cause a denial of service (memory consumption and named crash) via a large or infinite number of referrals.

Affected Nodes:

Affected Nodes:	Additional Information:
xx.xxx.xx.xxx:53	• Running DNS service • Product BIND exists -- BIND 9.8.2rc1-RedHat-9.8.2-0.23.rc1.el6_5.1 Vulnerable version of product BIND found -- BIND 9.8.2rc1-RedHat-9.8.2-0.23.rc1.el6_5.1

References:

Source	Reference
BID	71590
CERT-VN	264212
CVE	CVE-2014-8500
DEBIAN	DSA-3094
URL	https://kb.isc.org/article/AA-01216/0

Vulnerability Solution:

More information about upgrading your version of ISC BIND is available on the ISC website.

3.1.9. Remotely Exploitable Buffer Overflow in mod_ssl (http-mods-0003)

Description:

mod_ssl < 2.8.7 is vulnerable to a remotely exploitable buffer overflow when attempting to cache SSL sessions. This allows for remote code execution, and the modification of any file on the system.

Affected Nodes:

Affected Nodes:	Additional Information:
xx.xxx.xx.xxx:80	• Running HTTP service • Product HTTPD exists -- Apache HTTPD 2.2.24 Vulnerable version of component mod_ssl found -- mod_ssl 2.2.24
xx.xxx.xx.xxx:443	• Running HTTPS service • Product HTTPD exists -- Apache HTTPD 2.2.24 Vulnerable version of component mod_ssl found -- mod_ssl 2.2.24

References:

Source	Reference
BID	4189

Source	Reference
CALDERA	CSSA-2002-011.0
CONECTIVA	CLA-2002:465
CVE	CVE-2002-0082
DEBIAN	DSA-120
MANDRAKE	MDKSA-2002:020
REDHAT	RHSA-2002:041
REDHAT	RHSA-2002:042
REDHAT	RHSA-2002:045
URL	http://marc.theaimsgroup.com/?l=bugtraq&m=101518491916936&w=2
URL	http://www.apacheweek.com/issues/02-03-01#security
XF	8308

Vulnerability Solution:
Download and apply the upgrade from: http://www.modssl.org/
Upgrade to version 2.8.7 or later from the mod_ssl web site.

3.1.10. OpenSSL CMS structures with OriginatorInfo double free (CVE-2010-0742) (http-openssl-cve-2010-0742)

Description:

The Cryptographic Message Syntax (CMS) implementation in crypto/cms/cms_asn1.c in OpenSSL before 0.9.8o and 1.x before 1.0.0a does not properly handle structures that contain OriginatorInfo, which allows context-dependent attackers to modify invalid memory locations or conduct double-free attacks, and possibly execute arbitrary code, via unspecified vectors.

Affected Nodes:

Affected Nodes:	Additional Information:
xx.xxx.xx.xxx:80	• Running HTTP service Vulnerable version of component OpenSSL found -- OpenSSL 1.0.0-fips
xx.xxx.xx.xxx:443	• Running HTTPS service Vulnerable version of component OpenSSL found -- OpenSSL 1.0.0-fips

References:

Source	Reference
BID	40502
CVE	CVE-2010-0742
OVAL	OVAL12395
URL	http://www.openssl.org/news/secadv_20100601.txt

Vulnerability Solution:
- Upgrade to OpenSSL version 0.9.8o

Download and apply the upgrade from: http://ftp.openssl.org/source/openssl-0.9.8o.tar.gz
Upgrade to version 0.9.8o of OpenSSL. The source code for this release can be downloaded from OpenSSL's website. To obtain binaries for your platform, please visit your vendor's site. Please note that many operating system vendors choose to apply the most recent OpenSSL security patches to their distributions without changing the package version to the most recent OpenSSL version number.

- Upgrade to OpenSSL version 1.0.0a
  Download and apply the upgrade from: http://ftp.openssl.org/source/openssl-1.0.0a.tar.gz
  Upgrade to version 1.0.0a of OpenSSL. The source code for this release can be downloaded from OpenSSL's website. To obtain binaries for your platform, please visit your vendor's site. Please note that many operating system vendors choose to apply the most recent OpenSSL security patches to their distributions without changing the package version to the most recent OpenSSL version number.

3.1.11. OpenSSL ASN1 BIO vulnerability (CVE-2012-2110) (http-openssl-cve-2012-2110)

Description:

The asn1_d2i_read_bio function in crypto/asn1/a_d2i_fp.c in OpenSSL before 0.9.8v, 1.0.0 before 1.0.0i, and 1.0.1 before 1.0.1a does not properly interpret integer data, which allows remote attackers to conduct buffer overflow attacks, and cause a denial of service (memory corruption) or possibly have unspecified other impact, via crafted DER data, as demonstrated by an X.509 certificate or an RSA public key.

Affected Nodes:

Affected Nodes:	Additional Information:
xx.xxx.xx.xxx:80	• Running HTTP service Vulnerable version of component OpenSSL found -- OpenSSL 1.0.0-fips
xx.xxx.xx.xxx:443	• Running HTTPS service Vulnerable version of component OpenSSL found -- OpenSSL 1.0.0-fips

References:

Source	Reference
APPLE	APPLE-SA-2013-06-04-1
CVE	CVE-2012-2110
DEBIAN	DSA-2454
DISA_SEVERITY	Category I
DISA_VMSKEY	V0033884
IAVM	2012-A-0153
REDHAT	RHSA-2012:0518
REDHAT	RHSA-2012:0522
REDHAT	RHSA-2012:1306
REDHAT	RHSA-2012:1307
REDHAT	RHSA-2012:1308
URL	http://www.openssl.org/news/secadv_20120419.txt

Source	Reference
URL	http://www.openssl.org/news/secadv_20120424.txt

Vulnerability Solution:

- Upgrade to OpenSSL version 0.9.8v
  Download and apply the upgrade from: http://ftp.openssl.org/source/openssl-0.9.8v.tar.gz
  Upgrade to version 0.9.8v of OpenSSL. The source code for this release can be downloaded from OpenSSL's website. To obtain binaries for your platform, please visit your vendor's site. Please note that many operating system vendors choose to apply the most recent OpenSSL security patches to their distributions without changing the package version to the most recent OpenSSL version number.

- Upgrade to OpenSSL version 1.0.0i
  Download and apply the upgrade from: http://ftp.openssl.org/source/openssl-1.0.0i.tar.gz
  Upgrade to version 1.0.0i of OpenSSL. The source code for this release can be downloaded from OpenSSL's website. To obtain binaries for your platform, please visit your vendor's site. Please note that many operating system vendors choose to apply the most recent OpenSSL security patches to their distributions without changing the package version to the most recent OpenSSL version number.

- Upgrade to OpenSSL version 1.0.1a
  Download and apply the upgrade from: http://ftp.openssl.org/source/openssl-1.0.1a.tar.gz
  Upgrade to version 1.0.1a of OpenSSL. The source code for this release can be downloaded from OpenSSL's website. To obtain binaries for your platform, please visit your vendor's site. Please note that many operating system vendors choose to apply the most recent OpenSSL security patches to their distributions without changing the package version to the most recent OpenSSL version number.

3.1.12. OpenSSL (CVE-2015-0292) (http-openssl-cve-2015-0292)

Description:

Integer underflow in the EVP_DecodeUpdate function in crypto/evp/encode.c in the base64-decoding implementation in OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via crafted base64 data that triggers a buffer overflow.

Affected Nodes:

Affected Nodes:	Additional Information:
xx.xxx.xx.xxx:80	• Running HTTP service Vulnerable version of component OpenSSL found -- OpenSSL 1.0.0-fips
xx.xxx.xx.xxx:443	• Running HTTPS service Vulnerable version of component OpenSSL found -- OpenSSL 1.0.0-fips

References:

Source	Reference
BID	73228
CVE	CVE-2015-0292
DEBIAN	DSA-3197
REDHAT	RHSA-2015:0715
REDHAT	RHSA-2015:0716

Source	Reference
REDHAT	RHSA-2015:0752
REDHAT	RHSA-2015:0800
URL	http://www.openssl.org/news/secadv_20150319.txt

Vulnerability Solution:

- Upgrade to OpenSSL version 0.9.8za
  Download and apply the upgrade from: http://ftp.openssl.org/source/openssl-0.9.8za.tar.gz
  Upgrade to version 0.9.8za of OpenSSL. The source code for this release can be downloaded from OpenSSL's website. To obtain binaries for your platform, please visit your vendor's site. Please note that many operating system vendors choose to apply the most recent OpenSSL security patches to their distributions without changing the package version to the most recent OpenSSL version number.

- Upgrade to OpenSSL version 1.0.0m
  Download and apply the upgrade from: http://ftp.openssl.org/source/openssl-1.0.0m.tar.gz
  Upgrade to version 1.0.0m of OpenSSL. The source code for this release can be downloaded from OpenSSL's website. To obtain binaries for your platform, please visit your vendor's site. Please note that many operating system vendors choose to apply the most recent OpenSSL security patches to their distributions without changing the package version to the most recent OpenSSL version number.

- Upgrade to OpenSSL version 1.0.1h
  Download and apply the upgrade from: http://ftp.openssl.org/source/openssl-1.0.1h.tar.gz
  Upgrade to version 1.0.1h of OpenSSL. The source code for this release can be downloaded from OpenSSL's website. To obtain binaries for your platform, please visit your vendor's site. Please note that many operating system vendors choose to apply the most recent OpenSSL security patches to their distributions without changing the package version to the most recent OpenSSL version number.

3.2. Severe Vulnerabilities

3.2.1. Apache HTTPD: mod_status buffer overflow (CVE-2014-0226) (apache-httpd-cve-2014-0226)

Description:

The affected asset is vulnerable to this vulnerability ONLY if it is running one of the following modules: mod_status. Review your web server configuration for validation. A race condition was found in mod_status. An attacker able to access a public server status page on a server using a threaded MPM could send a carefully crafted request which could lead to a heap buffer overflow. Note that it is not a default or recommended configuration to have a public accessible server status page.

Affected Nodes:

Affected Nodes:	Additional Information:
xx.xxx.xx.xxx:80	• Running HTTP service • Product HTTPD exists -- Apache HTTPD 2.2.24 Vulnerable version of product HTTPD found -- Apache HTTPD 2.2.24
xx.xxx.xx.xxx:443	• Running HTTPS service • Product HTTPD exists -- Apache HTTPD 2.2.24 Vulnerable version of product HTTPD found -- Apache HTTPD 2.2.24

References:

Source	Reference

Source	Reference
APPLE	APPLE-SA-2015-04-08-2
BID	68678
CVE	CVE-2014-0226
DEBIAN	DSA-2989
DISA_SEVERITY	Category I
DISA_VMSKEY	V0053307
IAVM	2014-A-0114
OSVDB	109216
REDHAT	RHSA-2014:1019
REDHAT	RHSA-2014:1020
REDHAT	RHSA-2014:1021
URL	http://httpd.apache.org/security/vulnerabilities_22.html
URL	http://httpd.apache.org/security/vulnerabilities_24.html

Vulnerability Solution:

- Apache HTTPD >= 2.2 and < 2.2.29
  Upgrade to Apache HTTPD version 2.2.29
  Download and apply the upgrade from: http://archive.apache.org/dist/httpd/httpd-2.2.29.tar.gz
  Many platforms and distributions provide pre-built binary packages for Apache HTTP server. These pre-built packages are usually customized and optimized for a particular distribution, therefore we recommend that you use the packages if they are available for your operating system.

- Apache HTTPD >= 2.4 and < 2.4.10
  Upgrade to Apache HTTPD version 2.4.10
  Download and apply the upgrade from: http://archive.apache.org/dist/httpd/httpd-2.4.10.tar.gz
  Many platforms and distributions provide pre-built binary packages for Apache HTTP server. These pre-built packages are usually customized and optimized for a particular distribution, therefore we recommend that you use the packages if they are available for your operating system.

3.2.2. ISC BIND: BIND 9 with DNS64 enabled can unexpectedly terminate when resolving domains in RPZ (CVE-2012-5689) (dns-bind-cve-2012-5689)

Description:

ISC BIND 9.8.x through 9.8.4-P1 and 9.9.x through 9.9.2-P1, in certain configurations involving DNS64 with a Response Policy Zone that lacks an AAAA rewrite rule, allows remote attackers to cause a denial of service (assertion failure and named daemon exit) via a query for an AAAA record.

Affected Nodes:

Affected Nodes:	Additional Information:
xx.xxx.xx.xxx:53	• Running DNS service • Product BIND exists -- BIND 9.8.2rc1-RedHat-9.8.2-0.23.rc1.el6_5.1 Vulnerable version of product BIND found -- BIND

Affected Nodes:	Additional Information:
	9.8.2rc1-RedHat-9.8.2-0.23.rc1.el6_5.1

References:

Source	Reference
CVE	CVE-2012-5689
REDHAT	RHSA-2013:0550
URL	https://kb.isc.org/article/AA-00855/0
URL	https://kb.isc.org/article/AA-00855/74/CVE-2012-5689%3A-BIND-9-with-DNS64-enabled-can-unexpectedly-terminate-when-resolving-domains-in-RPZ.html

Vulnerability Solution:
More information about upgrading your version of ISC BIND is available on the ISC website.

3.2.3. FTP credentials transmitted unencrypted (ftp-plaintext-auth)

Description:

The server supports authentication methods in which credentials are sent in plaintext over unencrypted channels. If an attacker were to intercept traffic between a client and this server, the credentials would be exposed.

Affected Nodes:

Affected Nodes:	Additional Information:
xx.xxx.xx.xxx:21	• Running FTP service Configuration item ftp.plaintext.authentication set to 'true' matched

References:
None

Vulnerability Solution:
Disable plaintext authentication methods or enable encryption for the FTP service. Refer to the software's documentation for specific instructions.

3.2.4. OpenSSL Invalid TLS/DTLS record attack (CVE-2012-2333) (http-openssl-cve-2012-2333)

Description:

Integer underflow in OpenSSL before 0.9.8x, 1.0.0 before 1.0.0j, and 1.0.1 before 1.0.1c, when TLS 1.1, TLS 1.2, or DTLS is used with CBC encryption, allows remote attackers to cause a denial of service (buffer over-read) or possibly have unspecified other impact via a crafted TLS packet that is not properly handled during a certain explicit IV calculation.

Affected Nodes:

Affected Nodes:	Additional Information:
xx.xxx.xx.xxx:80	• Running HTTP service Vulnerable version of component OpenSSL found -- OpenSSL 1.0.0-fips
xx.xxx.xx.xxx:443	• Running HTTPS service Vulnerable version of component OpenSSL found -- OpenSSL 1.0.0-fips

References:

Source	Reference
APPLE	APPLE-SA-2013-06-04-1
BID	53476
CERT-VN	737740
CVE	CVE-2012-2333
DEBIAN	DSA-2475
REDHAT	RHSA-2012:1306
REDHAT	RHSA-2012:1307
REDHAT	RHSA-2012:1308
URL	http://www.openssl.org/news/secadv_20120510.txt
XF	75525

Vulnerability Solution:

- Upgrade to OpenSSL version 0.9.8x
  Download and apply the upgrade from: http://ftp.openssl.org/source/openssl-0.9.8x.tar.gz
  Upgrade to version 0.9.8x of OpenSSL. The source code for this release can be downloaded from OpenSSL's website. To obtain binaries for your platform, please visit your vendor's site. Please note that many operating system vendors choose to apply the most recent OpenSSL security patches to their distributions without changing the package version to the most recent OpenSSL version number.

- Upgrade to OpenSSL version 1.0.0j
  Download and apply the upgrade from: http://ftp.openssl.org/source/openssl-1.0.0j.tar.gz
  Upgrade to version 1.0.0j of OpenSSL. The source code for this release can be downloaded from OpenSSL's website. To obtain binaries for your platform, please visit your vendor's site. Please note that many operating system vendors choose to apply the most recent OpenSSL security patches to their distributions without changing the package version to the most recent OpenSSL version number.

- Upgrade to OpenSSL version 1.0.1c
  Download and apply the upgrade from: http://ftp.openssl.org/source/openssl-1.0.1c.tar.gz
  Upgrade to version 1.0.1c of OpenSSL. The source code for this release can be downloaded from OpenSSL's website. To obtain binaries for your platform, please visit your vendor's site. Please note that many operating system vendors choose to apply the most recent OpenSSL security patches to their distributions without changing the package version to the most recent OpenSSL version number.

3.2.5. OpenSSL DTLS invalid fragment vulnerability (CVE-2014-0195) (http-openssl-cve-2014-0195)

Description:

The dtls1_reassemble_fragment function in d1_both.c in OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h does not properly validate fragment lengths in DTLS ClientHello messages, which allows remote attackers to execute arbitrary code or cause a denial of service (buffer overflow and application crash) via a long non-initial fragment.

Affected Nodes:

Affected Nodes:	Additional Information:
xx.xxx.xx.xxx:80	• Running HTTP service Vulnerable version of component OpenSSL found -- OpenSSL 1.0.0-fips
xx.xxx.xx.xxx:443	• Running HTTPS service Vulnerable version of component OpenSSL found -- OpenSSL 1.0.0-fips

References:

Source	Reference
CVE	CVE-2014-0195
DISA_SEVERITY	Category I
DISA_VMSKEY	V0052625
DISA_VMSKEY	V0052627
DISA_VMSKEY	V0052637
DISA_VMSKEY	V0052641
DISA_VMSKEY	V0053203
DISA_VMSKEY	V0054749
IAVM	2014-A-0087
IAVM	2014-A-0099
IAVM	2014-A-0140
IAVM	2014-B-0077
IAVM	2014-B-0079
IAVM	2014-B-0080
URL	http://www.openssl.org/news/secadv_20140605.txt

Vulnerability Solution:

- Upgrade to OpenSSL version 0.9.8za
  Download and apply the upgrade from: http://ftp.openssl.org/source/openssl-0.9.8za.tar.gz
  Upgrade to version 0.9.8za of OpenSSL. The source code for this release can be downloaded from OpenSSL's website. To obtain binaries for your platform, please visit your vendor's site. Please note that many operating system vendors choose to apply the most recent OpenSSL security patches to their distributions without changing the package version to the most recent OpenSSL version number.

- Upgrade to OpenSSL version 1.0.0m
  Download and apply the upgrade from: http://ftp.openssl.org/source/openssl-1.0.0m.tar.gz
  Upgrade to version 1.0.0m of OpenSSL. The source code for this release can be downloaded from OpenSSL's website. To obtain binaries for your platform, please visit your vendor's site. Please note that many operating system vendors choose to apply the most recent OpenSSL security patches to their distributions without changing the package version to the most recent OpenSSL version number.

- Upgrade to OpenSSL version 1.0.1h
  Download and apply the upgrade from: http://ftp.openssl.org/source/openssl-1.0.1h.tar.gz
  Upgrade to version 1.0.1h of OpenSSL. The source code for this release can be downloaded from OpenSSL's website. To obtain binaries for your platform, please visit your vendor's site. Please note that many operating system vendors choose to apply the most recent OpenSSL security patches to their distributions without changing the package version to the most recent OpenSSL version

number.

3.2.6. OpenSSL SSL/TLS MITM vulnerability (CVE-2014-0224) (http-openssl-cve-2014-0224)

Description:

OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h does not properly restrict processing of ChangeCipherSpec messages, which allows man-in-the-middle attackers to trigger use of a zero-length master key in certain OpenSSL-to-OpenSSL communications, and consequently hijack sessions or obtain sensitive information, via a crafted TLS handshake, aka the "CCS Injection" vulnerability.

Affected Nodes:

Affected Nodes:	Additional Information:
xx.xxx.xx.xxx:80	• Running HTTP service Vulnerable version of component OpenSSL found -- OpenSSL 1.0.0-fips
xx.xxx.xx.xxx:443	• Running HTTPS service Vulnerable version of component OpenSSL found -- OpenSSL 1.0.0-fips

References:

Source	Reference
CERT-VN	978508
CVE	CVE-2014-0224
DISA_SEVERITY	Category I
DISA_VMSKEY	V0052625
DISA_VMSKEY	V0052627
DISA_VMSKEY	V0052637
DISA_VMSKEY	V0052639
DISA_VMSKEY	V0052641
DISA_VMSKEY	V0052893
DISA_VMSKEY	V0052901
DISA_VMSKEY	V0052907
DISA_VMSKEY	V0052909
DISA_VMSKEY	V0052911
DISA_VMSKEY	V0053179
DISA_VMSKEY	V0053181
DISA_VMSKEY	V0053183
DISA_VMSKEY	V0053319
DISA_VMSKEY	V0053501

Source	Reference
DISA_VMSKEY	V0053505
DISA_VMSKEY	V0053507
DISA_VMSKEY	V0053509
DISA_VMSKEY	V0054749
DISA_VMSKEY	V0055451
DISA_VMSKEY	V0055459
DISA_VMSKEY	V0055461
IAVM	2014-A-0087
IAVM	2014-A-0109
IAVM	2014-A-0110
IAVM	2014-A-0111
IAVM	2014-A-0115
IAVM	2014-A-0140
IAVM	2014-A-0159
IAVM	2014-A-0163
IAVM	2014-A-0164
IAVM	2014-B-0077
IAVM	2014-B-0078
IAVM	2014-B-0079
IAVM	2014-B-0080
IAVM	2014-B-0084
IAVM	2014-B-0088
IAVM	2014-B-0089
IAVM	2014-B-0091
IAVM	2014-B-0092
IAVM	2014-B-0097
IAVM	2014-B-0101
IAVM	2014-B-0102
IAVM	2014-B-0103
REDHAT	RHSA-2014:0624
REDHAT	RHSA-2014:0626
REDHAT	RHSA-2014:0627

Source	Reference
REDHAT	RHSA-2014:0630
REDHAT	RHSA-2014:0631
REDHAT	RHSA-2014:0632
REDHAT	RHSA-2014:0633
REDHAT	RHSA-2014:0680
URL	http://www.openssl.org/news/secadv_20140605.txt

Vulnerability Solution:

- Upgrade to OpenSSL version 0.9.8za
  Download and apply the upgrade from: http://ftp.openssl.org/source/openssl-0.9.8za.tar.gz
  Upgrade to version 0.9.8za of OpenSSL. The source code for this release can be downloaded from OpenSSL's website. To obtain binaries for your platform, please visit your vendor's site. Please note that many operating system vendors choose to apply the most recent OpenSSL security patches to their distributions without changing the package version to the most recent OpenSSL version number.

- Upgrade to OpenSSL version 1.0.0m
  Download and apply the upgrade from: http://ftp.openssl.org/source/openssl-1.0.0m.tar.gz
  Upgrade to version 1.0.0m of OpenSSL. The source code for this release can be downloaded from OpenSSL's website. To obtain binaries for your platform, please visit your vendor's site. Please note that many operating system vendors choose to apply the most recent OpenSSL security patches to their distributions without changing the package version to the most recent OpenSSL version number.

- Upgrade to OpenSSL version 1.0.1h
  Download and apply the upgrade from: http://ftp.openssl.org/source/openssl-1.0.1h.tar.gz
  Upgrade to version 1.0.1h of OpenSSL. The source code for this release can be downloaded from OpenSSL's website. To obtain binaries for your platform, please visit your vendor's site. Please note that many operating system vendors choose to apply the most recent OpenSSL security patches to their distributions without changing the package version to the most recent OpenSSL version number.

3.2.7. OpenSSL (CVE-2014-3509) (http-openssl-cve-2014-3509)

Description:

Race condition in the ssl_parse_serverhello_tlsext function in t1_lib.c in OpenSSL 1.0.0 before 1.0.0n and 1.0.1 before 1.0.1i, when multithreading and session resumption are used, allows remote SSL servers to cause a denial of service (memory overwrite and client application crash) or possibly have unspecified other impact by sending Elliptic Curve (EC) Supported Point Formats Extension data.

Affected Nodes:

Affected Nodes:	Additional Information:
xx.xxx.xx.xxx:80	• Running HTTP service Vulnerable version of component OpenSSL found -- OpenSSL 1.0.0-fips
xx.xxx.xx.xxx:443	• Running HTTPS service Vulnerable version of component OpenSSL found -- OpenSSL 1.0.0-fips

References:

Source	Reference

Source	Reference
CVE	CVE-2014-3509
DEBIAN	DSA-2998
DISA_SEVERITY	Category I
DISA_VMSKEY	V0053793
IAVM	2014-A-0122
NETBSD	NetBSD-SA2014-008
REDHAT	RHSA-2015:0197
URL	http://www.openssl.org/news/secadv_20140806.txt

Vulnerability Solution:

- Upgrade to OpenSSL version 1.0.0n
  Download and apply the upgrade from: http://ftp.openssl.org/source/openssl-1.0.0n.tar.gz
  Upgrade to version 1.0.0n of OpenSSL. The source code for this release can be downloaded from OpenSSL's website. To obtain binaries for your platform, please visit your vendor's site. Please note that many operating system vendors choose to apply the most recent OpenSSL security patches to their distributions without changing the package version to the most recent OpenSSL version number.

- Upgrade to OpenSSL version 1.0.1i
  Download and apply the upgrade from: http://ftp.openssl.org/source/openssl-1.0.1i.tar.gz
  Upgrade to version 1.0.1i of OpenSSL. The source code for this release can be downloaded from OpenSSL's website. To obtain binaries for your platform, please visit your vendor's site. Please note that many operating system vendors choose to apply the most recent OpenSSL security patches to their distributions without changing the package version to the most recent OpenSSL version number.

3.2.8. OpenSSL (CVE-2014-3567) (http-openssl-cve-2014-3567)

Description:

Memory leak in the tls_decrypt_ticket function in t1_lib.c in OpenSSL before 0.9.8zc, 1.0.0 before 1.0.0o, and 1.0.1 before 1.0.1j allows remote attackers to cause a denial of service (memory consumption) via a crafted session ticket that triggers an integrity-check failure.

Affected Nodes:

Affected Nodes:	Additional Information:
xx.xxx.xx.xxx:80	• Running HTTP service Vulnerable version of component OpenSSL found -- OpenSSL 1.0.0-fips
xx.xxx.xx.xxx:443	• Running HTTPS service Vulnerable version of component OpenSSL found -- OpenSSL 1.0.0-fips

References:

Source	Reference
APPLE	APPLE-SA-2015-01-27-4
BID	70586
CVE	CVE-2014-3567

Source	Reference
DEBIAN	DSA-3053
NETBSD	NetBSD-SA2014-015
REDHAT	RHSA-2014:1652
REDHAT	RHSA-2014:1692
REDHAT	RHSA-2015:0126
URL	http://www.openssl.org/news/secadv_20141015.txt

Vulnerability Solution:

- Upgrade to OpenSSL version 0.9.8zc
  Download and apply the upgrade from: http://ftp.openssl.org/source/openssl-0.9.8zc.tar.gz
  Upgrade to version 0.9.8zc of OpenSSL. The source code for this release can be downloaded from OpenSSL's website. To obtain binaries for your platform, please visit your vendor's site. Please note that many operating system vendors choose to apply the most recent OpenSSL security patches to their distributions without changing the package version to the most recent OpenSSL version number.

- Upgrade to OpenSSL version 1.0.0o
  Download and apply the upgrade from: http://ftp.openssl.org/source/openssl-1.0.0o.tar.gz
  Upgrade to version 1.0.0o of OpenSSL. The source code for this release can be downloaded from OpenSSL's website. To obtain binaries for your platform, please visit your vendor's site. Please note that many operating system vendors choose to apply the most recent OpenSSL security patches to their distributions without changing the package version to the most recent OpenSSL version number.

- Upgrade to OpenSSL version 1.0.1j
  Download and apply the upgrade from: http://ftp.openssl.org/source/openssl-1.0.1j.tar.gz
  Upgrade to version 1.0.1j of OpenSSL. The source code for this release can be downloaded from OpenSSL's website. To obtain binaries for your platform, please visit your vendor's site. Please note that many operating system vendors choose to apply the most recent OpenSSL security patches to their distributions without changing the package version to the most recent OpenSSL version number.

3.2.9. OpenSSL (CVE-2015-0209) (http-openssl-cve-2015-0209)

Description:

Use-after-free vulnerability in the d2i_ECPrivateKey function in crypto/ec/ec_asn1.c in OpenSSL before 0.9.8zf, 1.0.0 before 1.0.0r, 1.0.1 before 1.0.1m, and 1.0.2 before 1.0.2a might allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly have unspecified other impact via a malformed Elliptic Curve (EC) private-key file that is improperly handled during import.

Affected Nodes:

Affected Nodes:	Additional Information:
xx.xxx.xx.xxx:80	• Running HTTP service Vulnerable version of component OpenSSL found -- OpenSSL 1.0.0-fips
xx.xxx.xx.xxx:443	• Running HTTPS service Vulnerable version of component OpenSSL found -- OpenSSL 1.0.0-fips

References:

Source	Reference

Source	Reference
CVE	CVE-2015-0209
DEBIAN	DSA-3197
REDHAT	RHSA-2015:0715
REDHAT	RHSA-2015:0716
REDHAT	RHSA-2015:0752
URL	http://www.openssl.org/news/secadv_20150319.txt

Vulnerability Solution:

- Upgrade to OpenSSL version 0.9.8zf
  Download and apply the upgrade from: http://ftp.openssl.org/source/openssl-0.9.8zf.tar.gz
  Upgrade to version 0.9.8zf of OpenSSL. The source code for this release can be downloaded from OpenSSL's website. To obtain binaries for your platform, please visit your vendor's site. Please note that many operating system vendors choose to apply the most recent OpenSSL security patches to their distributions without changing the package version to the most recent OpenSSL version number.

- Upgrade to OpenSSL version 1.0.0r
  Download and apply the upgrade from: http://ftp.openssl.org/source/openssl-1.0.0r.tar.gz
  Upgrade to version 1.0.0r of OpenSSL. The source code for this release can be downloaded from OpenSSL's website. To obtain binaries for your platform, please visit your vendor's site. Please note that many operating system vendors choose to apply the most recent OpenSSL security patches to their distributions without changing the package version to the most recent OpenSSL version number.

- Upgrade to OpenSSL version 1.0.1m
  Download and apply the upgrade from: http://ftp.openssl.org/source/openssl-1.0.1m.tar.gz
  Upgrade to version 1.0.1m of OpenSSL. The source code for this release can be downloaded from OpenSSL's website. To obtain binaries for your platform, please visit your vendor's site. Please note that many operating system vendors choose to apply the most recent OpenSSL security patches to their distributions without changing the package version to the most recent OpenSSL version number.

- Upgrade to OpenSSL version 1.0.2a
  Download and apply the upgrade from: http://ftp.openssl.org/source/openssl-1.0.2a.tar.gz
  Upgrade to version 1.0.2a of OpenSSL. The source code for this release can be downloaded from OpenSSL's website. To obtain binaries for your platform, please visit your vendor's site. Please note that many operating system vendors choose to apply the most recent OpenSSL security patches to their distributions without changing the package version to the most recent OpenSSL version number.

3.2.10. SMTP credentials transmitted unencrypted (smtp-plaintext-auth)

Description:

The server supports authentication methods where credentials are sent in plaintext over unencrypted channels. If an attacker can intercept traffic between a client and this server, the credentials would be exposed.

Affected Nodes:

Affected Nodes:	Additional Information:
xx.xxx.xx.xxx:587	• Running SMTP service Configuration item smtp.plaintext.authentication set to 'true' matched

References:
None

Vulnerability Solution:
Follow the product-specific documentation to disable plaintext authentication methods for the SMTP service.

3.2.11. OpenSSL pkey_rsa_verifyrecover uninitialized buffer information leak (CVE-2010-1633) (http-openssl-cve-2010-1633)

Description:

RSA verification recovery in the EVP_PKEY_verify_recover function in OpenSSL 1.x before 1.0.0a, as used by pkeyutl and possibly other applications, returns uninitialized memory upon failure, which might allow context-dependent attackers to bypass intended key requirements or obtain sensitive information via unspecified vectors. NOTE: some of these details are obtained from third party information.

Affected Nodes:

Affected Nodes:	Additional Information:
xx.xxx.xx.xxx:80	• Running HTTP service Vulnerable version of component OpenSSL found -- OpenSSL 1.0.0-fips
xx.xxx.xx.xxx:443	• Running HTTPS service Vulnerable version of component OpenSSL found -- OpenSSL 1.0.0-fips

References:

Source	Reference
BID	40503
CVE	CVE-2010-1633
URL	http://www.openssl.org/news/secadv_20100601.txt

Vulnerability Solution:
Download and apply the upgrade from: http://ftp.openssl.org/source/openssl-1.0.0a.tar.gz
Upgrade to version 1.0.0a of OpenSSL. The source code for this release can be downloaded from OpenSSL's website. To obtain binaries for your platform, please visit your vendor's site. Please note that many operating system vendors choose to apply the most recent OpenSSL security patches to their distributions without changing the package version to the most recent OpenSSL version number.

3.2.12. OpenSSL (CVE-2013-6450) (http-openssl-cve-2013-6450)

Description:

The DTLS retransmission implementation in OpenSSL 1.0.0 before 1.0.0l and 1.0.1 before 1.0.1f does not properly maintain data structures for digest and encryption contexts, which might allow man-in-the-middle attackers to trigger the use of a different context and cause a denial of service (application crash) by interfering with packet delivery, related to ssl/d1_both.c and ssl/t1_enc.c.

Affected Nodes:

Affected Nodes:	Additional Information:
xx.xxx.xx.xxx:80	• Running HTTP service Vulnerable version of component OpenSSL found -- OpenSSL 1.0.0-fips
xx.xxx.xx.xxx:443	• Running HTTPS service

Affected Nodes:	Additional Information:
	Vulnerable version of component OpenSSL found -- OpenSSL 1.0.0-fips

References:

Source	Reference
BID	64618
CVE	CVE-2013-6450
DEBIAN	DSA-2833
REDHAT	RHSA-2014:0015

Vulnerability Solution:

- Upgrade to OpenSSL version 1.0.0l
  Download and apply the upgrade from: http://ftp.openssl.org/source/openssl-1.0.0l.tar.gz
  Upgrade to version 1.0.0l of OpenSSL. The source code for this release can be downloaded from OpenSSL's website. To obtain binaries for your platform, please visit your vendor's site. Please note that many operating system vendors choose to apply the most recent OpenSSL security patches to their distributions without changing the package version to the most recent OpenSSL version number.

- Upgrade to OpenSSL version 1.0.1f
  Download and apply the upgrade from: http://ftp.openssl.org/source/openssl-1.0.1f.tar.gz
  Upgrade to version 1.0.1f of OpenSSL. The source code for this release can be downloaded from OpenSSL's website. To obtain binaries for your platform, please visit your vendor's site. Please note that many operating system vendors choose to apply the most recent OpenSSL security patches to their distributions without changing the package version to the most recent OpenSSL version number.

3.2.13. HTTP TRACE Method Enabled (http-trace-method-enabled)

Description:

The HTTP TRACE method is normally used to return the full HTTP request back to the requesting client for proxy-debugging purposes. An attacker can create a webpage using XMLHTTP, ActiveX, or XMLDOM to cause a client to issue a TRACE request and capture the client's cookies. This effectively results in a Cross-Site Scripting attack.

Affected Nodes:

Affected Nodes:	Additional Information:
xx.xxx.xx.xxx:80	Running HTTP serviceHTTP TRACE request to http://Xx.xxx.xx.xxx/ 3: TRACE / HTTP/1.1 4: Host: Xx.xxx.xx.xxx 3: Cookie: vulnerable=yes
xx.xxx.xx.xxx:443	Running HTTPS serviceHTTP TRACE request to https://Xx.xxx.xx.xxx/ 3: TRACE / HTTP/1.1 4: Host: Xx.xxx.xx.xxx:443 3: Cookie: vulnerable=yes

References:

Source	Reference
APPLE	APPLE-SA-2009-11-09-1
BID	15222
BID	19915
BID	24456
BID	36956
BID	9506
CERT-VN	867593
CVE	CVE-2004-2320
CVE	CVE-2004-2763
CVE	CVE-2005-3398
CVE	CVE-2006-4683
CVE	CVE-2007-3008
CVE	CVE-2008-7253
CVE	CVE-2009-2823
CVE	CVE-2010-0386
DISA_SEVERITY	Category II
DISA_VMSKEY	V0011706
IAVM	2005-T-0043
OSVDB	35511
OSVDB	3726
OVAL	OVAL1445
URL	http://www.apacheweek.com/issues/03-01-24#news
URL	http://www.kb.cert.org/vuls/id/867593
XF	14959
XF	34854

Vulnerability Solution:

- Apache HTTPD
  Disable HTTP TRACE Method for Apache
  Newer versions of Apache (1.3.34 and 2.0.55 and later) provide a configuration directive called TraceEnable. To deny TRACE requests, add the following line to the server configuration:
  ```
  TraceEnable off
  ```
  For older versions of the Apache webserver, use the mod_rewrite module to deny the TRACE requests:
  ```
  RewriteEngine On
  RewriteCond %{REQUEST_METHOD} ^TRACE
  RewriteRule .* - [F]
  ```

- IIS, PWS, Microsoft-IIS, Internet Information Services, Internet Information Services, Microsoft-PWS
  Disable HTTP TRACE Method for Microsoft IIS
  For Microsoft Internet Information Services (IIS), you may use the URLScan tool, freely available at
  http://www.microsoft.com/technet/security/tools/urlscan.mspx

- Java System Web Server, SunONE WebServer, Sun-ONE-Web-Server, iPlanet
  Disable HTTP TRACE Method for SunONE/iPlanet

- For Sun ONE/iPlanet Web Server v6.0 SP2 and later, add the following configuration to the top of the default object in the 'obj.conf' file:
  ```
  <Client method="TRACE">
     AuthTrans fn="set-variable"
        remove-headers="transfer-encoding"
        set-headers="content-length: -1"
        error="501"
  </Client>
  ```
  You must then restart the server for the changes to take effect.

- For Sun ONE/iPlanet Web Server prior to v6.0 SP2, follow the instructions provided the 'Relief/Workaround' section of Sun's official advisory: http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert%2F50603

- Lotus Domino
  Disable HTTP TRACE Method for Domino
  Follow IBM's instructions for disabling HTTP methods on the Domino server by adding the following line to the server's NOTES.INI file:
  ```
  HTTPDisableMethods=TRACE
  ```
  After saving NOTES.INI, restart the Notes web server by issuing the console command "tell http restart".

3.2.14. Untrusted TLS/SSL server X.509 certificate (tls-untrusted-ca)

Description:

The server's TLS/SSL certificate is signed by a Certification Authority (CA) that is not a well-known, trusted one. It could indicate that a TLS/SSL man-in-the-middle is taking place and is eavesdropping on TLS/SSL connections.

Affected Nodes:

Affected Nodes:	Additional Information:
xx.xxx.xx.xxx:587	TLS/SSL certificate signed by xxxxxxxx, untrusted CA: CN=GeoTrust SSL CA - G3, O=GeoTrust Inc., C=US -- Path does not chain with any of the trust anchors.
xx.xxx.xx.xxx:993	TLS/SSL certificate signed by xxxxxxxx, untrusted CA: CN=GeoTrust SSL CA - G3, O=GeoTrust Inc., C=US -- basic constraints check failed: pathLenConstraint violated - this cert must be the last cert in the certification path.
xx.xxx.xx.xxx:995	TLS/SSL certificate signed by xxxxxxxx, untrusted CA: CN=GeoTrust SSL CA - G3, O=GeoTrust Inc., C=US -- basic constraints check failed: pathLenConstraint violated - this cert must be the last cert in the certification path.

References:
None

Vulnerability Solution:
Obtain a new certificate signed by a trusted CA, such as Thawte or Verisign.

The exact instructions for obtaining a new certificate depend on your organization's requirements. Generally, you will need to generate a certificate request and save the request as a file. This file is then sent to a Certificate Authority (CA) for processing. After you have received a new certificate file from the Certificate Authority, you will have to install it on the TLS/SSL server. The exact instructions for installing a certificate differ for each product. Follow their documentation.

3.2.15. Apache HTTPD: mod_rewrite log escape filtering (CVE-2013-1862) (apache-httpd-cve-2013-1862)

Description:

The affected asset is vulnerable to this vulnerability ONLY if it is running one of the following modules: mod_rewrite. Review your web server configuration for validation. mod_rewrite does not filter terminal escape sequences from logs, which could make it easier for attackers to insert those sequences into terminal emulators containing vulnerabilities related to escape sequences.

Affected Nodes:

Affected Nodes:	Additional Information:
xx.xxx.xx.xxx:80	• Running HTTP service • Product HTTPD exists -- Apache HTTPD 2.2.24 Vulnerable version of product HTTPD found -- Apache HTTPD 2.2.24
xx.xxx.xx.xxx:443	• Running HTTPS service • Product HTTPD exists -- Apache HTTPD 2.2.24 Vulnerable version of product HTTPD found -- Apache HTTPD 2.2.24

References:

Source	Reference
BID	64758
CVE	CVE-2013-1862
DISA_SEVERITY	Category I
DISA_VMSKEY	V0040288
IAVM	2013-A-0177
OVAL	OVAL18790
OVAL	OVAL19534
REDHAT	RHSA-2013:0815
REDHAT	RHSA-2013:1207
REDHAT	RHSA-2013:1208
REDHAT	RHSA-2013:1209
URL	http://httpd.apache.org/security/vulnerabilities_20.html
URL	http://httpd.apache.org/security/vulnerabilities_22.html

Vulnerability Solution:

- Apache HTTPD >= 2.0 and < 2.0.65
  Upgrade to Apache HTTPD version 2.0.65
  Download and apply the upgrade from: http://archive.apache.org/dist/httpd/httpd-2.0.65.tar.gz
  Many platforms and distributions provide pre-built binary packages for Apache HTTP server. These pre-built packages are usually customized and optimized for a particular distribution, therefore we recommend that you use the packages if they are available for

your operating system.

- Apache HTTPD >= 2.2 and < 2.2.25
  Upgrade to Apache HTTPD version 2.2.25
  Download and apply the upgrade from: http://archive.apache.org/dist/httpd/httpd-2.2.25.tar.gz
  Many platforms and distributions provide pre-built binary packages for Apache HTTP server. These pre-built packages are usually customized and optimized for a particular distribution, therefore we recommend that you use the packages if they are available for your operating system.

3.2.16. Apache HTTPD: HTTP Trailers processing bypass (CVE-2013-5704) (apache-httpd-cve-2013-5704)

Description:

HTTP trailers could be used to replace HTTP headers late during request processing, potentially undoing or otherwise confusing modules that examined or modified request headers earlier. This fix adds the "MergeTrailers" directive to restore legacy behavior.

Affected Nodes:

Affected Nodes:	Additional Information:
xx.xxx.xx.xxx:80	• Running HTTP service • Product HTTPD exists -- Apache HTTPD 2.2.24 Vulnerable version of product HTTPD found -- Apache HTTPD 2.2.24
xx.xxx.xx.xxx:443	• Running HTTPS service • Product HTTPD exists -- Apache HTTPD 2.2.24 Vulnerable version of product HTTPD found -- Apache HTTPD 2.2.24

References:

Source	Reference
APPLE	APPLE-SA-2015-04-08-2
BID	66550
CVE	CVE-2013-5704
REDHAT	RHSA-2015:0325
URL	http://httpd.apache.org/security/vulnerabilities_22.html
URL	http://httpd.apache.org/security/vulnerabilities_24.html

Vulnerability Solution:

- Apache HTTPD >= 2.2 and < 2.2.29
  Upgrade to Apache HTTPD version 2.2.29
  Download and apply the upgrade from: http://archive.apache.org/dist/httpd/httpd-2.2.29.tar.gz
  Many platforms and distributions provide pre-built binary packages for Apache HTTP server. These pre-built packages are usually customized and optimized for a particular distribution, therefore we recommend that you use the packages if they are available for your operating system.

- Apache HTTPD >= 2.4 and < 2.4.12
  Upgrade to Apache HTTPD version 2.4.12
  Download and apply the upgrade from: http://archive.apache.org/dist/httpd/httpd-2.4.12.tar.gz
  Many platforms and distributions provide pre-built binary packages for Apache HTTP server. These pre-built packages are usually customized and optimized for a particular distribution, therefore we recommend that you use the packages if they are available for your operating system.

3.2.17. Apache HTTPD: mod_dav crash (CVE-2013-6438) (apache-httpd-cve-2013-6438)

Description:

The affected asset is vulnerable to this vulnerability ONLY if it is running one of the following modules: mod_dav. Review your web server configuration for validation. XML parsing code in mod_dav incorrectly calculates the end of the string when removing leading spaces and places a NUL character outside the buffer, causing random crashes. This XML parsing code is only used with DAV provider modules that support DeltaV, of which the only publicly released provider is mod_dav_svn.

Affected Nodes:

Affected Nodes:	Additional Information:
xx.xxx.xx.xxx:80	• Running HTTP service • Product HTTPD exists -- Apache HTTPD 2.2.24 Vulnerable version of product HTTPD found -- Apache HTTPD 2.2.24
xx.xxx.xx.xxx:443	• Running HTTPS service • Product HTTPD exists -- Apache HTTPD 2.2.24 Vulnerable version of product HTTPD found -- Apache HTTPD 2.2.24

References:

Source	Reference
APPLE	APPLE-SA-2014-10-16-1
APPLE	APPLE-SA-2015-04-08-2
BID	66303
CVE	CVE-2013-6438
URL	http://httpd.apache.org/security/vulnerabilities_22.html
URL	http://httpd.apache.org/security/vulnerabilities_24.html

Vulnerability Solution:

- Apache HTTPD >= 2.2 and < 2.2.27
  Upgrade to Apache HTTPD version 2.2.27
  Download and apply the upgrade from: http://archive.apache.org/dist/httpd/httpd-2.2.27.tar.gz
  Many platforms and distributions provide pre-built binary packages for Apache HTTP server. These pre-built packages are usually customized and optimized for a particular distribution, therefore we recommend that you use the packages if they are available for your operating system.

- Apache HTTPD >= 2.4 and < 2.4.9
  Upgrade to Apache HTTPD version 2.4.9
  Download and apply the upgrade from: http://archive.apache.org/dist/httpd/httpd-2.4.9.tar.gz
  Many platforms and distributions provide pre-built binary packages for Apache HTTP server. These pre-built packages are usually customized and optimized for a particular distribution, therefore we recommend that you use the packages if they are available for your operating system.

3.2.18. Apache HTTPD: mod_log_config crash (CVE-2014-0098) (apache-httpd-cve-2014-0098)

Description:

The affected asset is vulnerable to this vulnerability ONLY if it is running one of the following modules: mod_log_config. Review your web server configuration for validation. A flaw was found in mod_log_config. A remote attacker could send a specific truncated cookie causing a crash. This crash would only be a denial of service if using a threaded MPM.

Affected Nodes:

Affected Nodes:	Additional Information:
xx.xxx.xx.xxx:80	• Running HTTP service • Product HTTPD exists -- Apache HTTPD 2.2.24 Vulnerable version of product HTTPD found -- Apache HTTPD 2.2.24
xx.xxx.xx.xxx:443	• Running HTTPS service • Product HTTPD exists -- Apache HTTPD 2.2.24 Vulnerable version of product HTTPD found -- Apache HTTPD 2.2.24

References:

Source	Reference
APPLE	APPLE-SA-2014-10-16-1
APPLE	APPLE-SA-2015-04-08-2
BID	66303
CVE	CVE-2014-0098
URL	http://httpd.apache.org/security/vulnerabilities_22.html
URL	http://httpd.apache.org/security/vulnerabilities_24.html

Vulnerability Solution:

- Apache HTTPD >= 2.2 and < 2.2.27
  Upgrade to Apache HTTPD version 2.2.27
  Download and apply the upgrade from: http://archive.apache.org/dist/httpd/httpd-2.2.27.tar.gz
  Many platforms and distributions provide pre-built binary packages for Apache HTTP server. These pre-built packages are usually customized and optimized for a particular distribution, therefore we recommend that you use the packages if they are available for your operating system.

- Apache HTTPD >= 2.4 and < 2.4.9
  Upgrade to Apache HTTPD version 2.4.9
  Download and apply the upgrade from: http://archive.apache.org/dist/httpd/httpd-2.4.9.tar.gz
  Many platforms and distributions provide pre-built binary packages for Apache HTTP server. These pre-built packages are usually customized and optimized for a particular distribution, therefore we recommend that you use the packages if they are available for your operating system.

3.2.19. Apache HTTPD: mod_cgid denial of service (CVE-2014-0231) (apache-httpd-cve-2014-0231)

Description:

The affected asset is vulnerable to this vulnerability ONLY if it is running one of the following modules: mod_cgid. Review your web server configuration for validation. A flaw was found in mod_cgid. If a server using mod_cgid hosted CGI scripts which did not consume standard input, a remote attacker could cause child processes to hang indefinitely, leading to denial of service.

Affected Nodes:

Affected Nodes:	Additional Information:
xx.xxx.xx.xxx:80	• Running HTTP service • Product HTTPD exists -- Apache HTTPD 2.2.24 Vulnerable version of product HTTPD found -- Apache HTTPD 2.2.24
xx.xxx.xx.xxx:443	• Running HTTPS service • Product HTTPD exists -- Apache HTTPD 2.2.24 Vulnerable version of product HTTPD found -- Apache HTTPD 2.2.24

References:

Source	Reference
APPLE	APPLE-SA-2015-04-08-2
BID	68742
CVE	CVE-2014-0231
DEBIAN	DSA-2989
DISA_SEVERITY	Category I
DISA_VMSKEY	V0053307
IAVM	2014-A-0114
REDHAT	RHSA-2014:1019
REDHAT	RHSA-2014:1020
REDHAT	RHSA-2014:1021
URL	http://httpd.apache.org/security/vulnerabilities_22.html
URL	http://httpd.apache.org/security/vulnerabilities_24.html

Vulnerability Solution:

- Apache HTTPD >= 2.2 and < 2.2.29
  Upgrade to Apache HTTPD version 2.2.29
  Download and apply the upgrade from: http://archive.apache.org/dist/httpd/httpd-2.2.29.tar.gz
  Many platforms and distributions provide pre-built binary packages for Apache HTTP server. These pre-built packages are usually customized and optimized for a particular distribution, therefore we recommend that you use the packages if they are available for your operating system.

- Apache HTTPD >= 2.4 and < 2.4.10
  Upgrade to Apache HTTPD version 2.4.10
  Download and apply the upgrade from: http://archive.apache.org/dist/httpd/httpd-2.4.10.tar.gz
  Many platforms and distributions provide pre-built binary packages for Apache HTTP server. These pre-built packages are usually customized and optimized for a particular distribution, therefore we recommend that you use the packages if they are available for your operating system.

3.2.20. Database Open Access (database-open-access)

Description:

The database allows any remote system the ability to connect to it. It is recommended to limit direct access to trusted systems because databases may contain sensitive data, and new vulnerabilities and exploits are discovered routinely for them. For this reason, it is a violation of PCI DSS section 1.3.7 to have databases listening on ports accessible from the Internet, even when protected with

secure authentication mechanisms.

Affected Nodes:

Affected Nodes:	Additional Information:
xx.xxx.xx.xxx:3306	Running MySQL service

References:

Source	Reference
URL	https://www.pcisecuritystandards.org/security_standards/download.html?id=pci_dss_v1-2.pdf

Vulnerability Solution:

Configure the database server to only allow access to trusted systems. For example, the PCI DSS standard requires you to place the database in an internal network zone, segregated from the DMZ

3.2.21. ISC BIND: A Problem with Trust Anchor Management Can Cause named to Crash (CVE-2015-1349) (dns-bind-cve-2015-1349)

Description:

named in ISC BIND 9.7.0 through 9.9.6 before 9.9.6-P2 and 9.10.x before 9.10.1-P2, when DNSSEC validation and the managed-keys feature are enabled, allows remote attackers to cause a denial of service (assertion failure and daemon exit, or daemon crash) by triggering an incorrect trust-anchor management scenario in which no key is ready for use.

Affected Nodes:

Affected Nodes:	Additional Information:
xx.xxx.xx.xxx:53	• Running DNS service • Product BIND exists -- BIND 9.8.2rc1-RedHat-9.8.2-0.23.rc1.el6_5.1 Vulnerable version of product BIND found -- BIND 9.8.2rc1-RedHat-9.8.2-0.23.rc1.el6_5.1

References:

Source	Reference
CVE	CVE-2015-1349
REDHAT	RHSA-2015:0672
URL	https://kb.isc.org/article/AA-01235/0

Vulnerability Solution:

More information about upgrading your version of ISC BIND is available on the ISC website.

3.2.22. mod_ssl Directive Mapping Buffer Overflow (http-mods-0008)

Description:

There exists an off-by-one buffer overflow vulnerability in mod_ssl < 2.8.10 in the compatability functionality (directive mapping). The impact of this vulnerability is xxxxxxxx.

Affected Nodes:

Affected Nodes:	Additional Information:
xx.xxx.xx.xxx:80	• Running HTTP service • Product HTTPD exists -- Apache HTTPD 2.2.24 Vulnerable version of component mod_ssl found -- mod_ssl 2.2.24
xx.xxx.xx.xxx:443	• Running HTTPS service • Product HTTPD exists -- Apache HTTPD 2.2.24 Vulnerable version of component mod_ssl found -- mod_ssl 2.2.24

References:

Source	Reference
BID	5084
CALDERA	CSSA-2002-031.0
CONECTIVA	CLA-2002:504
CVE	CVE-2002-0653
DEBIAN	DSA-135
MANDRAKE	MDKSA-2002:048
REDHAT	RHSA-2002:134
REDHAT	RHSA-2002:135
REDHAT	RHSA-2002:136
REDHAT	RHSA-2002:146
REDHAT	RHSA-2002:164
REDHAT	RHSA-2003:106
SUSE	SuSE-SA:2002:028
URL	http://marc.theaimsgroup.com/?l=apache-modssl&m=102491918531562
XF	9415

Vulnerability Solution:

Download and apply the upgrade from: http://www.modssl.org/source/OBSOLETE/mod_ssl-2.8.10-1.3.26.tar.gz
Upgrade to v2.8.10 or later.

3.2.23. OpenSSL OCSP stapling vulnerability (CVE-2011-0014) (http-openssl-cve-2011-0014)

Description:

ssl/t1_lib.c in OpenSSL 0.9.8h through 0.9.8q and 1.0.0 through 1.0.0c allows remote attackers to cause a denial of service (crash), and possibly obtain sensitive information in applications that use OpenSSL, via a malformed ClientHello handshake message that triggers an out-of-bounds memory access, aka "OCSP stapling vulnerability."

Affected Nodes:

Affected Nodes:	Additional Information:

Affected Nodes:	Additional Information:
xx.xxx.xx.xxx:80	• Running HTTP service Vulnerable version of component OpenSSL found -- OpenSSL 1.0.0-fips
xx.xxx.xx.xxx:443	• Running HTTPS service Vulnerable version of component OpenSSL found -- OpenSSL 1.0.0-fips

References:

Source	Reference
APPLE	APPLE-SA-2011-06-23-1
BID	46264
CVE	CVE-2011-0014
DEBIAN	DSA-2162
DISA_SEVERITY	Category I
DISA_VMSKEY	V0033794
DISA_VMSKEY	V0033884
IAVM	2012-A-0148
IAVM	2012-A-0153
NETBSD	NetBSD-SA2011-002
OSVDB	70847
OVAL	OVAL18985
REDHAT	RHSA-2011:0677
URL	http://www.openssl.org/news/secadv_20110208.txt

Vulnerability Solution:

- Upgrade to OpenSSL version 0.9.8r
  Download and apply the upgrade from: http://ftp.openssl.org/source/openssl-0.9.8r.tar.gz
  Upgrade to version 0.9.8r of OpenSSL. The source code for this release can be downloaded from OpenSSL's website. To obtain binaries for your platform, please visit your vendor's site. Please note that many operating system vendors choose to apply the most recent OpenSSL security patches to their distributions without changing the package version to the most recent OpenSSL version number.

- Upgrade to OpenSSL version 1.0.0d
  Download and apply the upgrade from: http://ftp.openssl.org/source/openssl-1.0.0d.tar.gz
  Upgrade to version 1.0.0d of OpenSSL. The source code for this release can be downloaded from OpenSSL's website. To obtain binaries for your platform, please visit your vendor's site. Please note that many operating system vendors choose to apply the most recent OpenSSL security patches to their distributions without changing the package version to the most recent OpenSSL version number.

3.2.24. OpenSSL CRL verification vulnerability in OpenSSL (CVE-2011-3207) (http-openssl-cve-2011-3207)

Description:

crypto/x509/x509_vfy.c in OpenSSL 1.0.x before 1.0.0e does not initialize certain structure members, which makes it easier for remote

attackers to bypass CRL validation by using a nextUpdate value corresponding to a time in the past.

Affected Nodes:

Affected Nodes:	Additional Information:
xx.xxx.xx.xxx:80	• Running HTTP service Vulnerable version of component OpenSSL found -- OpenSSL 1.0.0-fips
xx.xxx.xx.xxx:443	• Running HTTPS service Vulnerable version of component OpenSSL found -- OpenSSL 1.0.0-fips

References:

Source	Reference
APPLE	APPLE-SA-2013-06-04-1
CVE	CVE-2011-3207
REDHAT	RHSA-2011:1409
URL	http://www.openssl.org/news/secadv_20110906.txt

Vulnerability Solution:

Download and apply the upgrade from: http://ftp.openssl.org/source/openssl-1.0.0e.tar.gz
Upgrade to version 1.0.0e of OpenSSL. The source code for this release can be downloaded from OpenSSL's website. To obtain binaries for your platform, please visit your vendor's site. Please note that many operating system vendors choose to apply the most recent OpenSSL security patches to their distributions without changing the package version to the most recent OpenSSL version number.

3.2.25. OpenSSL TLS ephemeral ECDH crashes in OpenSSL (CVE-2011-3210) (http-openssl-cve-2011-3210)

Description:

The ephemeral ECDH ciphersuite functionality in OpenSSL 0.9.8 through 0.9.8r and 1.0.x before 1.0.0e does not ensure thread safety during processing of handshake messages from clients, which allows remote attackers to cause a denial of service (daemon crash) via out-of-order messages that violate the TLS protocol.

Affected Nodes:

Affected Nodes:	Additional Information:
xx.xxx.xx.xxx:80	• Running HTTP service Vulnerable version of component OpenSSL found -- OpenSSL 1.0.0-fips
xx.xxx.xx.xxx:443	• Running HTTPS service Vulnerable version of component OpenSSL found -- OpenSSL 1.0.0-fips

References:

Source	Reference
APPLE	APPLE-SA-2013-06-04-1
CVE	CVE-2011-3210
URL	http://www.openssl.org/news/secadv_20110906.txt

Vulnerability Solution:
Download and apply the upgrade from: http://ftp.openssl.org/source/openssl-1.0.0e.tar.gz
Upgrade to version 1.0.0e of OpenSSL. The source code for this release can be downloaded from OpenSSL's website. To obtain binaries for your platform, please visit your vendor's site. Please note that many operating system vendors choose to apply the most recent OpenSSL security patches to their distributions without changing the package version to the most recent OpenSSL version number.

3.2.26. OpenSSL memory leak caused by uncleared block cipher padding in SSL 3.0 records (CVE-2011-4576) (http-openssl-cve-2011-4576)

Description:

The SSL 3.0 implementation in OpenSSL before 0.9.8s and 1.x before 1.0.0f does not properly initialize data structures for block cipher padding, which might allow remote attackers to obtain sensitive information by decrypting the padding data sent by an SSL peer.

Affected Nodes:

Affected Nodes:	Additional Information:
xx.xxx.xx.xxx:80	• Running HTTP service Vulnerable version of component OpenSSL found -- OpenSSL 1.0.0-fips
xx.xxx.xx.xxx:443	• Running HTTPS service Vulnerable version of component OpenSSL found -- OpenSSL 1.0.0-fips

References:

Source	Reference
APPLE	APPLE-SA-2013-06-04-1
CERT-VN	737740
CVE	CVE-2011-4576
DEBIAN	DSA-2390
DISA_SEVERITY	Category I
DISA_VMSKEY	V0033794
DISA_VMSKEY	V0033884
DISA_VMSKEY	V0036639
IAVM	2012-A-0148
IAVM	2012-A-0153
IAVM	2013-A-0027
REDHAT	RHSA-2012:1306
REDHAT	RHSA-2012:1307
REDHAT	RHSA-2012:1308
URL	http://www.openssl.org/news/secadv_20120104.txt

Vulnerability Solution:
- Upgrade to OpenSSL version 0.9.8s

Download and apply the upgrade from: http://ftp.openssl.org/source/openssl-0.9.8s.tar.gz
Upgrade to version 0.9.8s of OpenSSL. The source code for this release can be downloaded from OpenSSL's website. To obtain binaries for your platform, please visit your vendor's site. Please note that many operating system vendors choose to apply the most recent OpenSSL security patches to their distributions without changing the package version to the most recent OpenSSL version number.

- Upgrade to OpenSSL version 1.0.0f
  Download and apply the upgrade from: http://ftp.openssl.org/source/openssl-1.0.0f.tar.gz
  Upgrade to version 1.0.0f of OpenSSL. The source code for this release can be downloaded from OpenSSL's website. To obtain binaries for your platform, please visit your vendor's site. Please note that many operating system vendors choose to apply the most recent OpenSSL security patches to their distributions without changing the package version to the most recent OpenSSL version number.

3.2.27. OpenSSL server gated cryptography (SGC) denial of service via handshake restarts (CVE-2011-4619) (http-openssl-cve-2011-4619)

Description:

The Server Gated Cryptography (SGC) implementation in OpenSSL before 0.9.8s and 1.x before 1.0.0f does not properly handle handshake restarts, which allows remote attackers to cause a denial of service (CPU consumption) via unspecified vectors.

Affected Nodes:

Affected Nodes:	Additional Information:
xx.xxx.xx.xxx:80	• Running HTTP service Vulnerable version of component OpenSSL found -- OpenSSL 1.0.0-fips
xx.xxx.xx.xxx:443	• Running HTTPS service Vulnerable version of component OpenSSL found -- OpenSSL 1.0.0-fips

References:

Source	Reference
APPLE	APPLE-SA-2013-06-04-1
CERT-VN	737740
CVE	CVE-2011-4619
DEBIAN	DSA-2390
DISA_SEVERITY	Category I
DISA_VMSKEY	V0033794
DISA_VMSKEY	V0033884
DISA_VMSKEY	V0036639
IAVM	2012-A-0148
IAVM	2012-A-0153
IAVM	2013-A-0027
REDHAT	RHSA-2012:1306
REDHAT	RHSA-2012:1307

Source	Reference
REDHAT	RHSA-2012:1308
URL	http://www.openssl.org/news/secadv_20120104.txt

Vulnerability Solution:

- Upgrade to OpenSSL version 0.9.8s
  Download and apply the upgrade from: http://ftp.openssl.org/source/openssl-0.9.8s.tar.gz
  Upgrade to version 0.9.8s of OpenSSL. The source code for this release can be downloaded from OpenSSL's website. To obtain binaries for your platform, please visit your vendor's site. Please note that many operating system vendors choose to apply the most recent OpenSSL security patches to their distributions without changing the package version to the most recent OpenSSL version number.

- Upgrade to OpenSSL version 1.0.0f
  Download and apply the upgrade from: http://ftp.openssl.org/source/openssl-1.0.0f.tar.gz
  Upgrade to version 1.0.0f of OpenSSL. The source code for this release can be downloaded from OpenSSL's website. To obtain binaries for your platform, please visit your vendor's site. Please note that many operating system vendors choose to apply the most recent OpenSSL security patches to their distributions without changing the package version to the most recent OpenSSL version number.

3.2.28. OpenSSL TLS denial of service caused by invalid GOST parameters (CVE-2012-0027) (http-openssl-cve-2012-0027)

Description:

The GOST ENGINE in OpenSSL before 1.0.0f does not properly handle invalid parameters for the GOST block cipher, which allows remote attackers to cause a denial of service (daemon crash) via crafted data from a TLS client.

Affected Nodes:

Affected Nodes:	Additional Information:
xx.xxx.xx.xxx:80	• Running HTTP service Vulnerable version of component OpenSSL found -- OpenSSL 1.0.0-fips
xx.xxx.xx.xxx:443	• Running HTTPS service Vulnerable version of component OpenSSL found -- OpenSSL 1.0.0-fips

References:

Source	Reference
CVE	CVE-2012-0027
OSVDB	78191
URL	http://www.openssl.org/news/secadv_20120104.txt

Vulnerability Solution:

Download and apply the upgrade from: http://ftp.openssl.org/source/openssl-1.0.0f.tar.gz
Upgrade to version 1.0.0f of OpenSSL. The source code for this release can be downloaded from OpenSSL's website. To obtain binaries for your platform, please visit your vendor's site. Please note that many operating system vendors choose to apply the most recent OpenSSL security patches to their distributions without changing the package version to the most recent OpenSSL version number.

3.2.29. OpenSSL CMS and S/MIME Bleichenbacher attack (CVE-2012-0884) (http-openssl-cve-2012-0884)

Description:

The implementation of Cryptographic Message Syntax (CMS) and PKCS #7 in OpenSSL before 0.9.8u and 1.x before 1.0.0h does not properly restrict certain oracle behavior, which makes it easier for context-dependent attackers to decrypt data via a Million Message Attack (MMA) adaptive chosen ciphertext attack.

Affected Nodes:

Affected Nodes:	Additional Information:
xx.xxx.xx.xxx:80	• Running HTTP service Vulnerable version of component OpenSSL found -- OpenSSL 1.0.0-fips
xx.xxx.xx.xxx:443	• Running HTTPS service Vulnerable version of component OpenSSL found -- OpenSSL 1.0.0-fips

References:

Source	Reference
CERT-VN	737740
CVE	CVE-2012-0884
DEBIAN	DSA-2454
REDHAT	RHSA-2012:0488
REDHAT	RHSA-2012:0531
REDHAT	RHSA-2012:1306
REDHAT	RHSA-2012:1307
REDHAT	RHSA-2012:1308
URL	http://www.openssl.org/news/secadv_20120312.txt

Vulnerability Solution:

- Upgrade to OpenSSL version 0.9.8u
  Download and apply the upgrade from: http://ftp.openssl.org/source/openssl-0.9.8u.tar.gz
  Upgrade to version 0.9.8u of OpenSSL. The source code for this release can be downloaded from OpenSSL's website. To obtain binaries for your platform, please visit your vendor's site. Please note that many operating system vendors choose to apply the most recent OpenSSL security patches to their distributions without changing the package version to the most recent OpenSSL version number.

- Upgrade to OpenSSL version 1.0.0h
  Download and apply the upgrade from: http://ftp.openssl.org/source/openssl-1.0.0h.tar.gz
  Upgrade to version 1.0.0h of OpenSSL. The source code for this release can be downloaded from OpenSSL's website. To obtain binaries for your platform, please visit your vendor's site. Please note that many operating system vendors choose to apply the most recent OpenSSL security patches to their distributions without changing the package version to the most recent OpenSSL version number.

3.2.30. OpenSSL (CVE-2013-0166) (http-openssl-cve-2013-0166)

Description:

OpenSSL before 0.9.8y, 1.0.0 before 1.0.0k, and 1.0.1 before 1.0.1d does not properly perform signature verification for OCSP

responses, which allows remote OCSP servers to cause a denial of service (NULL pointer dereference and application crash) via an invalid key.

Affected Nodes:

Affected Nodes:	Additional Information:
xx.xxx.xx.xxx:80	• Running HTTP service Vulnerable version of component OpenSSL found -- OpenSSL 1.0.0-fips
xx.xxx.xx.xxx:443	• Running HTTPS service Vulnerable version of component OpenSSL found -- OpenSSL 1.0.0-fips

References:

Source	Reference
APPLE	APPLE-SA-2013-09-12-1
CERT-VN	737740
CVE	CVE-2013-0166
DEBIAN	DSA-2621
OVAL	OVAL18754
OVAL	OVAL19081
OVAL	OVAL19360
OVAL	OVAL19487
REDHAT	RHSA-2013:0587
REDHAT	RHSA-2013:0782
REDHAT	RHSA-2013:0783
REDHAT	RHSA-2013:0833
URL	http://www.openssl.org/news/secadv_20130205.txt

Vulnerability Solution:

- Upgrade to OpenSSL version 0.9.8y
  Download and apply the upgrade from: http://ftp.openssl.org/source/openssl-0.9.8y.tar.gz
  Upgrade to version 0.9.8y of OpenSSL. The source code for this release can be downloaded from OpenSSL's website. To obtain binaries for your platform, please visit your vendor's site. Please note that many operating system vendors choose to apply the most recent OpenSSL security patches to their distributions without changing the package version to the most recent OpenSSL version number.

- Upgrade to OpenSSL version 1.0.0k
  Download and apply the upgrade from: http://ftp.openssl.org/source/openssl-1.0.0k.tar.gz
  Upgrade to version 1.0.0k of OpenSSL. The source code for this release can be downloaded from OpenSSL's website. To obtain binaries for your platform, please visit your vendor's site. Please note that many operating system vendors choose to apply the most recent OpenSSL security patches to their distributions without changing the package version to the most recent OpenSSL version number.

- Upgrade to OpenSSL version 1.0.1d
  Download and apply the upgrade from: http://ftp.openssl.org/source/openssl-1.0.1d.tar.gz
  Upgrade to version 1.0.1d of OpenSSL. The source code for this release can be downloaded from OpenSSL's website. To obtain

binaries for your platform, please visit your vendor's site. Please note that many operating system vendors choose to apply the most recent OpenSSL security patches to their distributions without changing the package version to the most recent OpenSSL version number.

3.2.31. OpenSSL (CVE-2014-3505) (http-openssl-cve-2014-3505)

Description:

Double free vulnerability in d1_both.c in the DTLS implementation in OpenSSL 0.9.8 before 0.9.8zb, 1.0.0 before 1.0.0n, and 1.0.1 before 1.0.1i allows remote attackers to cause a denial of service (application crash) via crafted DTLS packets that trigger an error condition.

Affected Nodes:

Affected Nodes:	Additional Information:
xx.xxx.xx.xxx:80	• Running HTTP service Vulnerable version of component OpenSSL found -- OpenSSL 1.0.0-fips
xx.xxx.xx.xxx:443	• Running HTTPS service Vulnerable version of component OpenSSL found -- OpenSSL 1.0.0-fips

References:

Source	Reference
CVE	CVE-2014-3505
DEBIAN	DSA-2998
DISA_SEVERITY	Category I
DISA_VMSKEY	V0053793
IAVM	2014-A-0122
NETBSD	NetBSD-SA2014-008
REDHAT	RHSA-2014:1256
REDHAT	RHSA-2014:1297
URL	http://www.openssl.org/news/secadv_20140806.txt

Vulnerability Solution:

- Upgrade to OpenSSL version 0.9.8zb
  Download and apply the upgrade from: http://ftp.openssl.org/source/openssl-0.9.8zb.tar.gz
  Upgrade to version 0.9.8zb of OpenSSL. The source code for this release can be downloaded from OpenSSL's website. To obtain binaries for your platform, please visit your vendor's site. Please note that many operating system vendors choose to apply the most recent OpenSSL security patches to their distributions without changing the package version to the most recent OpenSSL version number.

- Upgrade to OpenSSL version 1.0.0n
  Download and apply the upgrade from: http://ftp.openssl.org/source/openssl-1.0.0n.tar.gz
  Upgrade to version 1.0.0n of OpenSSL. The source code for this release can be downloaded from OpenSSL's website. To obtain binaries for your platform, please visit your vendor's site. Please note that many operating system vendors choose to apply the most recent OpenSSL security patches to their distributions without changing the package version to the most recent OpenSSL version number.

- Upgrade to OpenSSL version 1.0.1i
  Download and apply the upgrade from: http://ftp.openssl.org/source/openssl-1.0.1i.tar.gz
  Upgrade to version 1.0.1i of OpenSSL. The source code for this release can be downloaded from OpenSSL's website. To obtain binaries for your platform, please visit your vendor's site. Please note that many operating system vendors choose to apply the most recent OpenSSL security patches to their distributions without changing the package version to the most recent OpenSSL version number.

3.2.32. OpenSSL (CVE-2014-3506) (http-openssl-cve-2014-3506)

Description:

d1_both.c in the DTLS implementation in OpenSSL 0.9.8 before 0.9.8zb, 1.0.0 before 1.0.0n, and 1.0.1 before 1.0.1i allows remote attackers to cause a denial of service (memory consumption) via crafted DTLS handshake messages that trigger memory allocations corresponding to large length values.

Affected Nodes:

Affected Nodes:	Additional Information:
xx.xxx.xx.xxx:80	• Running HTTP service Vulnerable version of component OpenSSL found -- OpenSSL 1.0.0-fips
xx.xxx.xx.xxx:443	• Running HTTPS service Vulnerable version of component OpenSSL found -- OpenSSL 1.0.0-fips

References:

Source	Reference
CVE	CVE-2014-3506
DEBIAN	DSA-2998
DISA_SEVERITY	Category I
DISA_VMSKEY	V0053793
IAVM	2014-A-0122
NETBSD	NetBSD-SA2014-008
REDHAT	RHSA-2014:1256
REDHAT	RHSA-2014:1297
URL	http://www.openssl.org/news/secadv_20140806.txt

Vulnerability Solution:

- Upgrade to OpenSSL version 0.9.8zb
  Download and apply the upgrade from: http://ftp.openssl.org/source/openssl-0.9.8zb.tar.gz
  Upgrade to version 0.9.8zb of OpenSSL. The source code for this release can be downloaded from OpenSSL's website. To obtain binaries for your platform, please visit your vendor's site. Please note that many operating system vendors choose to apply the most recent OpenSSL security patches to their distributions without changing the package version to the most recent OpenSSL version number.

- Upgrade to OpenSSL version 1.0.0n
  Download and apply the upgrade from: http://ftp.openssl.org/source/openssl-1.0.0n.tar.gz
  Upgrade to version 1.0.0n of OpenSSL. The source code for this release can be downloaded from OpenSSL's website. To obtain

binaries for your platform, please visit your vendor's site. Please note that many operating system vendors choose to apply the most recent OpenSSL security patches to their distributions without changing the package version to the most recent OpenSSL version number.

- Upgrade to OpenSSL version 1.0.1i
  Download and apply the upgrade from: http://ftp.openssl.org/source/openssl-1.0.1i.tar.gz
  Upgrade to version 1.0.1i of OpenSSL. The source code for this release can be downloaded from OpenSSL's website. To obtain binaries for your platform, please visit your vendor's site. Please note that many operating system vendors choose to apply the most recent OpenSSL security patches to their distributions without changing the package version to the most recent OpenSSL version number.

3.2.33. OpenSSL (CVE-2014-3569) (http-openssl-cve-2014-3569)

Description:

The ssl23_get_client_hello function in s23_srvr.c in OpenSSL 0.9.8zc, 1.0.0o, and 1.0.1j does not properly handle attempts to use unsupported protocols, which allows remote attackers to cause a denial of service (NULL pointer dereference and daemon crash) via an unexpected handshake, as demonstrated by an SSLv3 handshake to a no-ssl3 application with certain error handling. NOTE: this issue became relevant after the CVE-2014-3568 fix.

Affected Nodes:

Affected Nodes:	Additional Information:
xx.xxx.xx.xxx:80	• Running HTTP service Vulnerable version of component OpenSSL found -- OpenSSL 1.0.0-fips
xx.xxx.xx.xxx:443	• Running HTTPS service Vulnerable version of component OpenSSL found -- OpenSSL 1.0.0-fips

References:

Source	Reference
APPLE	APPLE-SA-2015-04-08-2
BID	71934
CVE	CVE-2014-3569
DEBIAN	DSA-3125
URL	http://www.openssl.org/news/secadv_20150108.txt

Vulnerability Solution:

- Upgrade to OpenSSL version 0.9.8zd
  Download and apply the upgrade from: http://ftp.openssl.org/source/openssl-0.9.8zd.tar.gz
  Upgrade to version 0.9.8zd of OpenSSL. The source code for this release can be downloaded from OpenSSL's website. To obtain binaries for your platform, please visit your vendor's site. Please note that many operating system vendors choose to apply the most recent OpenSSL security patches to their distributions without changing the package version to the most recent OpenSSL version number.

- Upgrade to OpenSSL version 1.0.0p
  Download and apply the upgrade from: http://ftp.openssl.org/source/openssl-1.0.0p.tar.gz
  Upgrade to version 1.0.0p of OpenSSL. The source code for this release can be downloaded from OpenSSL's website. To obtain binaries for your platform, please visit your vendor's site. Please note that many operating system vendors choose to apply the most recent OpenSSL security patches to their distributions without changing the package version to the most recent OpenSSL version number.

- Upgrade to OpenSSL version 1.0.1k
  Download and apply the upgrade from: http://ftp.openssl.org/source/openssl-1.0.1k.tar.gz
  Upgrade to version 1.0.1k of OpenSSL. The source code for this release can be downloaded from OpenSSL's website. To obtain binaries for your platform, please visit your vendor's site. Please note that many operating system vendors choose to apply the most recent OpenSSL security patches to their distributions without changing the package version to the most recent OpenSSL version number.

3.2.34. OpenSSL (CVE-2014-3570) (http-openssl-cve-2014-3570)

Description:

The BN_sqr implementation in OpenSSL before 0.9.8zd, 1.0.0 before 1.0.0p, and 1.0.1 before 1.0.1k does not properly calculate the square of a BIGNUM value, which might make it easier for remote attackers to defeat cryptographic protection mechanisms via unspecified vectors, related to crypto/bn/asm/mips.pl, crypto/bn/asm/x86_64-gcc.c, and crypto/bn/bn_asm.c.

Affected Nodes:

Affected Nodes:	Additional Information:
xx.xxx.xx.xxx:80	• Running HTTP service Vulnerable version of component OpenSSL found -- OpenSSL 1.0.0-fips
xx.xxx.xx.xxx:443	• Running HTTPS service Vulnerable version of component OpenSSL found -- OpenSSL 1.0.0-fips

References:

Source	Reference
APPLE	APPLE-SA-2015-04-08-2
BID	71939
CVE	CVE-2014-3570
DEBIAN	DSA-3125
REDHAT	RHSA-2015:0066
REDHAT	RHSA-2015:0849
URL	http://www.openssl.org/news/secadv_20150108.txt

Vulnerability Solution:

- Upgrade to OpenSSL version 0.9.8zd
  Download and apply the upgrade from: http://ftp.openssl.org/source/openssl-0.9.8zd.tar.gz
  Upgrade to version 0.9.8zd of OpenSSL. The source code for this release can be downloaded from OpenSSL's website. To obtain binaries for your platform, please visit your vendor's site. Please note that many operating system vendors choose to apply the most recent OpenSSL security patches to their distributions without changing the package version to the most recent OpenSSL version number.

- Upgrade to OpenSSL version 1.0.0p
  Download and apply the upgrade from: http://ftp.openssl.org/source/openssl-1.0.0p.tar.gz
  Upgrade to version 1.0.0p of OpenSSL. The source code for this release can be downloaded from OpenSSL's website. To obtain binaries for your platform, please visit your vendor's site. Please note that many operating system vendors choose to apply the most recent OpenSSL security patches to their distributions without changing the package version to the most recent OpenSSL version number.

- Upgrade to OpenSSL version 1.0.1k
  Download and apply the upgrade from: http://ftp.openssl.org/source/openssl-1.0.1k.tar.gz
  Upgrade to version 1.0.1k of OpenSSL. The source code for this release can be downloaded from OpenSSL's website. To obtain binaries for your platform, please visit your vendor's site. Please note that many operating system vendors choose to apply the most recent OpenSSL security patches to their distributions without changing the package version to the most recent OpenSSL version number.

3.2.35. OpenSSL (CVE-2014-3571) (http-openssl-cve-2014-3571)

Description:

OpenSSL before 0.9.8zd, 1.0.0 before 1.0.0p, and 1.0.1 before 1.0.1k allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a crafted DTLS message that is processed with a different read operation for the handshake header than for the handshake body, related to the dtls1_get_record function in d1_pkt.c and the ssl3_read_n function in s3_pkt.c.

Affected Nodes:

Affected Nodes:	Additional Information:
xx.xxx.xx.xxx:80	• Running HTTP service Vulnerable version of component OpenSSL found -- OpenSSL 1.0.0-fips
xx.xxx.xx.xxx:443	• Running HTTPS service Vulnerable version of component OpenSSL found -- OpenSSL 1.0.0-fips

References:

Source	Reference
APPLE	APPLE-SA-2015-04-08-2
BID	71937
CVE	CVE-2014-3571
DEBIAN	DSA-3125
REDHAT	RHSA-2015:0066
URL	http://www.openssl.org/news/secadv_20150108.txt

Vulnerability Solution:

- Upgrade to OpenSSL version 0.9.8zd
  Download and apply the upgrade from: http://ftp.openssl.org/source/openssl-0.9.8zd.tar.gz
  Upgrade to version 0.9.8zd of OpenSSL. The source code for this release can be downloaded from OpenSSL's website. To obtain binaries for your platform, please visit your vendor's site. Please note that many operating system vendors choose to apply the most recent OpenSSL security patches to their distributions without changing the package version to the most recent OpenSSL version number.

- Upgrade to OpenSSL version 1.0.0p
  Download and apply the upgrade from: http://ftp.openssl.org/source/openssl-1.0.0p.tar.gz
  Upgrade to version 1.0.0p of OpenSSL. The source code for this release can be downloaded from OpenSSL's website. To obtain binaries for your platform, please visit your vendor's site. Please note that many operating system vendors choose to apply the most recent OpenSSL security patches to their distributions without changing the package version to the most recent OpenSSL version number.

- Upgrade to OpenSSL version 1.0.1k
  Download and apply the upgrade from: http://ftp.openssl.org/source/openssl-1.0.1k.tar.gz
  Upgrade to version 1.0.1k of OpenSSL. The source code for this release can be downloaded from OpenSSL's website. To obtain binaries for your platform, please visit your vendor's site. Please note that many operating system vendors choose to apply the most recent OpenSSL security patches to their distributions without changing the package version to the most recent OpenSSL version number.

3.2.36. OpenSSL (CVE-2014-3572) (http-openssl-cve-2014-3572)

Description:

The ssl3_get_key_exchange function in s3_clnt.c in OpenSSL before 0.9.8zd, 1.0.0 before 1.0.0p, and 1.0.1 before 1.0.1k allows remote SSL servers to conduct ECDHE-to-ECDH downgrade attacks and trigger a loss of forward secrecy by omitting the ServerKeyExchange message.

Affected Nodes:

Affected Nodes:	Additional Information:
xx.xxx.xx.xxx:80	• Running HTTP service Vulnerable version of component OpenSSL found -- OpenSSL 1.0.0-fips
xx.xxx.xx.xxx:443	• Running HTTPS service Vulnerable version of component OpenSSL found -- OpenSSL 1.0.0-fips

References:

Source	Reference
APPLE	APPLE-SA-2015-04-08-2
BID	71942
CVE	CVE-2014-3572
DEBIAN	DSA-3125
REDHAT	RHSA-2015:0066
URL	http://www.openssl.org/news/secadv_20150108.txt

Vulnerability Solution:

- Upgrade to OpenSSL version 0.9.8zd
  Download and apply the upgrade from: http://ftp.openssl.org/source/openssl-0.9.8zd.tar.gz
  Upgrade to version 0.9.8zd of OpenSSL. The source code for this release can be downloaded from OpenSSL's website. To obtain binaries for your platform, please visit your vendor's site. Please note that many operating system vendors choose to apply the most recent OpenSSL security patches to their distributions without changing the package version to the most recent OpenSSL version number.

- Upgrade to OpenSSL version 1.0.0p
  Download and apply the upgrade from: http://ftp.openssl.org/source/openssl-1.0.0p.tar.gz
  Upgrade to version 1.0.0p of OpenSSL. The source code for this release can be downloaded from OpenSSL's website. To obtain binaries for your platform, please visit your vendor's site. Please note that many operating system vendors choose to apply the most recent OpenSSL security patches to their distributions without changing the package version to the most recent OpenSSL version number.

- Upgrade to OpenSSL version 1.0.1k

Download and apply the upgrade from: http://ftp.openssl.org/source/openssl-1.0.1k.tar.gz
Upgrade to version 1.0.1k of OpenSSL. The source code for this release can be downloaded from OpenSSL's website. To obtain binaries for your platform, please visit your vendor's site. Please note that many operating system vendors choose to apply the most recent OpenSSL security patches to their distributions without changing the package version to the most recent OpenSSL version number.

3.2.37. OpenSSL (CVE-2014-8275) (http-openssl-cve-2014-8275)

Description:

OpenSSL before 0.9.8zd, 1.0.0 before 1.0.0p, and 1.0.1 before 1.0.1k does not enforce certain constraints on certificate data, which allows remote attackers to defeat a fingerprint-based certificate-blacklist protection mechanism by including crafted data within a certificate's unsigned portion, related to crypto/asn1/a_verify.c, crypto/dsa/dsa_asn1.c, crypto/ecdsa/ecs_vrf.c, and crypto/x509/x_all.c.

Affected Nodes:

Affected Nodes:	Additional Information:
xx.xxx.xx.xxx:80	• Running HTTP service Vulnerable version of component OpenSSL found -- OpenSSL 1.0.0-fips
xx.xxx.xx.xxx:443	• Running HTTPS service Vulnerable version of component OpenSSL found -- OpenSSL 1.0.0-fips

References:

Source	Reference
APPLE	APPLE-SA-2015-04-08-2
CVE	CVE-2014-8275
DEBIAN	DSA-3125
REDHAT	RHSA-2015:0066
REDHAT	RHSA-2015:0800
URL	http://www.openssl.org/news/secadv_20150108.txt

Vulnerability Solution:

- Upgrade to OpenSSL version 0.9.8zd
  Download and apply the upgrade from: http://ftp.openssl.org/source/openssl-0.9.8zd.tar.gz
  Upgrade to version 0.9.8zd of OpenSSL. The source code for this release can be downloaded from OpenSSL's website. To obtain binaries for your platform, please visit your vendor's site. Please note that many operating system vendors choose to apply the most recent OpenSSL security patches to their distributions without changing the package version to the most recent OpenSSL version number.

- Upgrade to OpenSSL version 1.0.0p
  Download and apply the upgrade from: http://ftp.openssl.org/source/openssl-1.0.0p.tar.gz
  Upgrade to version 1.0.0p of OpenSSL. The source code for this release can be downloaded from OpenSSL's website. To obtain binaries for your platform, please visit your vendor's site. Please note that many operating system vendors choose to apply the most recent OpenSSL security patches to their distributions without changing the package version to the most recent OpenSSL version number.

- Upgrade to OpenSSL version 1.0.1k
  Download and apply the upgrade from: http://ftp.openssl.org/source/openssl-1.0.1k.tar.gz
  Upgrade to version 1.0.1k of OpenSSL. The source code for this release can be downloaded from OpenSSL's website. To obtain

binaries for your platform, please visit your vendor's site. Please note that many operating system vendors choose to apply the most recent OpenSSL security patches to their distributions without changing the package version to the most recent OpenSSL version number.

3.2.38. OpenSSL (CVE-2015-0205) (http-openssl-cve-2015-0205)

Description:

The ssl3_get_cert_verify function in s3_srvr.c in OpenSSL 1.0.0 before 1.0.0p and 1.0.1 before 1.0.1k accepts client authentication with a Diffie-Hellman (DH) certificate without requiring a CertificateVerify message, which allows remote attackers to obtain access without knowledge of a private key via crafted TLS Handshake Protocol traffic to a server that recognizes a Certification Authority with DH support.

Affected Nodes:

Affected Nodes:	Additional Information:
xx.xxx.xx.xxx:80	• Running HTTP service Vulnerable version of component OpenSSL found -- OpenSSL 1.0.0-fips
xx.xxx.xx.xxx:443	• Running HTTPS service Vulnerable version of component OpenSSL found -- OpenSSL 1.0.0-fips

References:

Source	Reference
CVE	CVE-2015-0205
DEBIAN	DSA-3125
REDHAT	RHSA-2015:0066
URL	http://www.openssl.org/news/secadv_20150108.txt

Vulnerability Solution:

- Upgrade to OpenSSL version 1.0.0p
  Download and apply the upgrade from: http://ftp.openssl.org/source/openssl-1.0.0p.tar.gz
  Upgrade to version 1.0.0p of OpenSSL. The source code for this release can be downloaded from OpenSSL's website. To obtain binaries for your platform, please visit your vendor's site. Please note that many operating system vendors choose to apply the most recent OpenSSL security patches to their distributions without changing the package version to the most recent OpenSSL version number.

- Upgrade to OpenSSL version 1.0.1k
  Download and apply the upgrade from: http://ftp.openssl.org/source/openssl-1.0.1k.tar.gz
  Upgrade to version 1.0.1k of OpenSSL. The source code for this release can be downloaded from OpenSSL's website. To obtain binaries for your platform, please visit your vendor's site. Please note that many operating system vendors choose to apply the most recent OpenSSL security patches to their distributions without changing the package version to the most recent OpenSSL version number.

3.2.39. OpenSSL (CVE-2015-0206) (http-openssl-cve-2015-0206)

Description:

Memory leak in the dtls1_buffer_record function in d1_pkt.c in OpenSSL 1.0.0 before 1.0.0p and 1.0.1 before 1.0.1k allows remote attackers to cause a denial of service (memory consumption) by sending many duplicate records for the next epoch, leading to failure of replay detection.

Affected Nodes:

Affected Nodes:	Additional Information:
xx.xxx.xx.xxx:80	• Running HTTP service Vulnerable version of component OpenSSL found -- OpenSSL 1.0.0-fips
xx.xxx.xx.xxx:443	• Running HTTPS service Vulnerable version of component OpenSSL found -- OpenSSL 1.0.0-fips

References:

Source	Reference
CVE	CVE-2015-0206
DEBIAN	DSA-3125
REDHAT	RHSA-2015:0066
URL	http://www.openssl.org/news/secadv_20150108.txt

Vulnerability Solution:

- Upgrade to OpenSSL version 1.0.0p
  Download and apply the upgrade from: http://ftp.openssl.org/source/openssl-1.0.0p.tar.gz
  Upgrade to version 1.0.0p of OpenSSL. The source code for this release can be downloaded from OpenSSL's website. To obtain binaries for your platform, please visit your vendor's site. Please note that many operating system vendors choose to apply the most recent OpenSSL security patches to their distributions without changing the package version to the most recent OpenSSL version number.

- Upgrade to OpenSSL version 1.0.1k
  Download and apply the upgrade from: http://ftp.openssl.org/source/openssl-1.0.1k.tar.gz
  Upgrade to version 1.0.1k of OpenSSL. The source code for this release can be downloaded from OpenSSL's website. To obtain binaries for your platform, please visit your vendor's site. Please note that many operating system vendors choose to apply the most recent OpenSSL security patches to their distributions without changing the package version to the most recent OpenSSL version number.

3.2.40. OpenSSL (CVE-2015-0286) (http-openssl-cve-2015-0286)

Description:

The ASN1_TYPE_cmp function in crypto/asn1/a_type.c in OpenSSL before 0.9.8zf, 1.0.0 before 1.0.0r, 1.0.1 before 1.0.1m, and 1.0.2 before 1.0.2a does not properly perform boolean-type comparisons, which allows remote attackers to cause a denial of service (invalid read operation and application crash) via a crafted X.509 certificate to an endpoint that uses the certificate-verification feature.

Affected Nodes:

Affected Nodes:	Additional Information:
xx.xxx.xx.xxx:80	• Running HTTP service Vulnerable version of component OpenSSL found -- OpenSSL 1.0.0-fips
xx.xxx.xx.xxx:443	• Running HTTPS service Vulnerable version of component OpenSSL found -- OpenSSL 1.0.0-fips

References:

Source	Reference
BID	73225
CVE	CVE-2015-0286
DEBIAN	DSA-3197
REDHAT	RHSA-2015:0715
REDHAT	RHSA-2015:0716
REDHAT	RHSA-2015:0752
URL	http://www.openssl.org/news/secadv_20150319.txt

Vulnerability Solution:

- Upgrade to OpenSSL version 0.9.8zf
  Download and apply the upgrade from: http://ftp.openssl.org/source/openssl-0.9.8zf.tar.gz
  Upgrade to version 0.9.8zf of OpenSSL. The source code for this release can be downloaded from OpenSSL's website. To obtain binaries for your platform, please visit your vendor's site. Please note that many operating system vendors choose to apply the most recent OpenSSL security patches to their distributions without changing the package version to the most recent OpenSSL version number.

- Upgrade to OpenSSL version 1.0.0r
  Download and apply the upgrade from: http://ftp.openssl.org/source/openssl-1.0.0r.tar.gz
  Upgrade to version 1.0.0r of OpenSSL. The source code for this release can be downloaded from OpenSSL's website. To obtain binaries for your platform, please visit your vendor's site. Please note that many operating system vendors choose to apply the most recent OpenSSL security patches to their distributions without changing the package version to the most recent OpenSSL version number.

- Upgrade to OpenSSL version 1.0.1m
  Download and apply the upgrade from: http://ftp.openssl.org/source/openssl-1.0.1m.tar.gz
  Upgrade to version 1.0.1m of OpenSSL. The source code for this release can be downloaded from OpenSSL's website. To obtain binaries for your platform, please visit your vendor's site. Please note that many operating system vendors choose to apply the most recent OpenSSL security patches to their distributions without changing the package version to the most recent OpenSSL version number.

- Upgrade to OpenSSL version 1.0.2a
  Download and apply the upgrade from: http://ftp.openssl.org/source/openssl-1.0.2a.tar.gz
  Upgrade to version 1.0.2a of OpenSSL. The source code for this release can be downloaded from OpenSSL's website. To obtain binaries for your platform, please visit your vendor's site. Please note that many operating system vendors choose to apply the most recent OpenSSL security patches to their distributions without changing the package version to the most recent OpenSSL version number.

3.2.41. OpenSSL (CVE-2015-0287) (http-openssl-cve-2015-0287)

Description:

The ASN1_item_ex_d2i function in crypto/asn1/tasn_dec.c in OpenSSL before 0.9.8zf, 1.0.0 before 1.0.0r, 1.0.1 before 1.0.1m, and 1.0.2 before 1.0.2a does not reinitialize CHOICE and ADB data structures, which might allow attackers to cause a denial of service (invalid write operation and memory corruption) by leveraging an application that relies on ASN.1 structure reuse.

Affected Nodes:

Affected Nodes:	Additional Information:

Affected Nodes:	Additional Information:
xx.xxx.xx.xxx:80	• Running HTTP service Vulnerable version of component OpenSSL found -- OpenSSL 1.0.0-fips
xx.xxx.xx.xxx:443	• Running HTTPS service Vulnerable version of component OpenSSL found -- OpenSSL 1.0.0-fips

References:

Source	Reference
CVE	CVE-2015-0287
DEBIAN	DSA-3197
REDHAT	RHSA-2015:0715
REDHAT	RHSA-2015:0716
REDHAT	RHSA-2015:0752
REDHAT	RHSA-2015:0800
URL	http://www.openssl.org/news/secadv_20150319.txt

Vulnerability Solution:

- Upgrade to OpenSSL version 0.9.8zf
  Download and apply the upgrade from: http://ftp.openssl.org/source/openssl-0.9.8zf.tar.gz
  Upgrade to version 0.9.8zf of OpenSSL. The source code for this release can be downloaded from OpenSSL's website. To obtain binaries for your platform, please visit your vendor's site. Please note that many operating system vendors choose to apply the most recent OpenSSL security patches to their distributions without changing the package version to the most recent OpenSSL version number.

- Upgrade to OpenSSL version 1.0.0r
  Download and apply the upgrade from: http://ftp.openssl.org/source/openssl-1.0.0r.tar.gz
  Upgrade to version 1.0.0r of OpenSSL. The source code for this release can be downloaded from OpenSSL's website. To obtain binaries for your platform, please visit your vendor's site. Please note that many operating system vendors choose to apply the most recent OpenSSL security patches to their distributions without changing the package version to the most recent OpenSSL version number.

- Upgrade to OpenSSL version 1.0.1m
  Download and apply the upgrade from: http://ftp.openssl.org/source/openssl-1.0.1m.tar.gz
  Upgrade to version 1.0.1m of OpenSSL. The source code for this release can be downloaded from OpenSSL's website. To obtain binaries for your platform, please visit your vendor's site. Please note that many operating system vendors choose to apply the most recent OpenSSL security patches to their distributions without changing the package version to the most recent OpenSSL version number.

- Upgrade to OpenSSL version 1.0.2a
  Download and apply the upgrade from: http://ftp.openssl.org/source/openssl-1.0.2a.tar.gz
  Upgrade to version 1.0.2a of OpenSSL. The source code for this release can be downloaded from OpenSSL's website. To obtain binaries for your platform, please visit your vendor's site. Please note that many operating system vendors choose to apply the most recent OpenSSL security patches to their distributions without changing the package version to the most recent OpenSSL version number.

3.2.42. OpenSSL (CVE-2015-0288) (http-openssl-cve-2015-0288)

Description:

The X509_to_X509_REQ function in crypto/x509/x509_req.c in OpenSSL before 0.9.8zf, 1.0.0 before 1.0.0r, 1.0.1 before 1.0.1m, and 1.0.2 before 1.0.2a might allow attackers to cause a denial of service (NULL pointer dereference and application crash) via an invalid certificate key.

Affected Nodes:

Affected Nodes:	Additional Information:
xx.xxx.xx.xxx:80	• Running HTTP service Vulnerable version of component OpenSSL found -- OpenSSL 1.0.0-fips
xx.xxx.xx.xxx:443	• Running HTTPS service Vulnerable version of component OpenSSL found -- OpenSSL 1.0.0-fips

References:

Source	Reference
BID	73237
CVE	CVE-2015-0288
DEBIAN	DSA-3197
REDHAT	RHSA-2015:0715
REDHAT	RHSA-2015:0716
REDHAT	RHSA-2015:0752
REDHAT	RHSA-2015:0800
URL	http://www.openssl.org/news/secadv_20150319.txt

Vulnerability Solution:

- Upgrade to OpenSSL version 0.9.8zf
  Download and apply the upgrade from: http://ftp.openssl.org/source/openssl-0.9.8zf.tar.gz
  Upgrade to version 0.9.8zf of OpenSSL. The source code for this release can be downloaded from OpenSSL's website. To obtain binaries for your platform, please visit your vendor's site. Please note that many operating system vendors choose to apply the most recent OpenSSL security patches to their distributions without changing the package version to the most recent OpenSSL version number.

- Upgrade to OpenSSL version 1.0.0r
  Download and apply the upgrade from: http://ftp.openssl.org/source/openssl-1.0.0r.tar.gz
  Upgrade to version 1.0.0r of OpenSSL. The source code for this release can be downloaded from OpenSSL's website. To obtain binaries for your platform, please visit your vendor's site. Please note that many operating system vendors choose to apply the most recent OpenSSL security patches to their distributions without changing the package version to the most recent OpenSSL version number.

- Upgrade to OpenSSL version 1.0.1m
  Download and apply the upgrade from: http://ftp.openssl.org/source/openssl-1.0.1m.tar.gz
  Upgrade to version 1.0.1m of OpenSSL. The source code for this release can be downloaded from OpenSSL's website. To obtain binaries for your platform, please visit your vendor's site. Please note that many operating system vendors choose to apply the most recent OpenSSL security patches to their distributions without changing the package version to the most recent OpenSSL version number.

- Upgrade to OpenSSL version 1.0.2a
  Download and apply the upgrade from: http://ftp.openssl.org/source/openssl-1.0.2a.tar.gz
  Upgrade to version 1.0.2a of OpenSSL. The source code for this release can be downloaded from OpenSSL's website. To obtain

binaries for your platform, please visit your vendor's site. Please note that many operating system vendors choose to apply the most recent OpenSSL security patches to their distributions without changing the package version to the most recent OpenSSL version number.

3.2.43. OpenSSL (CVE-2015-0289) (http-openssl-cve-2015-0289)

Description:

The PKCS#7 implementation in OpenSSL before 0.9.8zf, 1.0.0 before 1.0.0r, 1.0.1 before 1.0.1m, and 1.0.2 before 1.0.2a does not properly handle a lack of outer ContentInfo, which allows attackers to cause a denial of service (NULL pointer dereference and application crash) by leveraging an application that processes arbitrary PKCS#7 data and providing malformed data with ASN.1 encoding, related to crypto/pkcs7/pk7_doit.c and crypto/pkcs7/pk7_lib.c.

Affected Nodes:

Affected Nodes:	Additional Information:
xx.xxx.xx.xxx:80	• Running HTTP service Vulnerable version of component OpenSSL found -- OpenSSL 1.0.0-fips
xx.xxx.xx.xxx:443	• Running HTTPS service Vulnerable version of component OpenSSL found -- OpenSSL 1.0.0-fips

References:

Source	Reference
CVE	CVE-2015-0289
DEBIAN	DSA-3197
REDHAT	RHSA-2015:0715
REDHAT	RHSA-2015:0716
REDHAT	RHSA-2015:0752
REDHAT	RHSA-2015:0800
URL	http://www.openssl.org/news/secadv_20150319.txt

Vulnerability Solution:

- Upgrade to OpenSSL version 0.9.8zf
  Download and apply the upgrade from: http://ftp.openssl.org/source/openssl-0.9.8zf.tar.gz
  Upgrade to version 0.9.8zf of OpenSSL. The source code for this release can be downloaded from OpenSSL's website. To obtain binaries for your platform, please visit your vendor's site. Please note that many operating system vendors choose to apply the most recent OpenSSL security patches to their distributions without changing the package version to the most recent OpenSSL version number.

- Upgrade to OpenSSL version 1.0.0r
  Download and apply the upgrade from: http://ftp.openssl.org/source/openssl-1.0.0r.tar.gz
  Upgrade to version 1.0.0r of OpenSSL. The source code for this release can be downloaded from OpenSSL's website. To obtain binaries for your platform, please visit your vendor's site. Please note that many operating system vendors choose to apply the most recent OpenSSL security patches to their distributions without changing the package version to the most recent OpenSSL version number.

- Upgrade to OpenSSL version 1.0.1m
  Download and apply the upgrade from: http://ftp.openssl.org/source/openssl-1.0.1m.tar.gz

Upgrade to version 1.0.1m of OpenSSL. The source code for this release can be downloaded from OpenSSL's website. To obtain binaries for your platform, please visit your vendor's site. Please note that many operating system vendors choose to apply the most recent OpenSSL security patches to their distributions without changing the package version to the most recent OpenSSL version number.

- Upgrade to OpenSSL version 1.0.2a
  Download and apply the upgrade from: http://ftp.openssl.org/source/openssl-1.0.2a.tar.gz
  Upgrade to version 1.0.2a of OpenSSL. The source code for this release can be downloaded from OpenSSL's website. To obtain binaries for your platform, please visit your vendor's site. Please note that many operating system vendors choose to apply the most recent OpenSSL security patches to their distributions without changing the package version to the most recent OpenSSL version number.

3.2.44. OpenSSL (CVE-2015-0293) (http-openssl-cve-2015-0293)

Description:

The SSLv2 implementation in OpenSSL before 0.9.8zf, 1.0.0 before 1.0.0r, 1.0.1 before 1.0.1m, and 1.0.2 before 1.0.2a allows remote attackers to cause a denial of service (s2_lib.c assertion failure and daemon exit) via a crafted CLIENT-MASTER-KEY message.

Affected Nodes:

Affected Nodes:	Additional Information:
xx.xxx.xx.xxx:80	• Running HTTP service Vulnerable version of component OpenSSL found -- OpenSSL 1.0.0-fips
xx.xxx.xx.xxx:443	• Running HTTPS service Vulnerable version of component OpenSSL found -- OpenSSL 1.0.0-fips

References:

Source	Reference
CVE	CVE-2015-0293
REDHAT	RHSA-2015:0715
REDHAT	RHSA-2015:0716
REDHAT	RHSA-2015:0752
REDHAT	RHSA-2015:0800
URL	http://www.openssl.org/news/secadv_20150319.txt

Vulnerability Solution:

- Upgrade to OpenSSL version 0.9.8zf
  Download and apply the upgrade from: http://ftp.openssl.org/source/openssl-0.9.8zf.tar.gz
  Upgrade to version 0.9.8zf of OpenSSL. The source code for this release can be downloaded from OpenSSL's website. To obtain binaries for your platform, please visit your vendor's site. Please note that many operating system vendors choose to apply the most recent OpenSSL security patches to their distributions without changing the package version to the most recent OpenSSL version number.

- Upgrade to OpenSSL version 1.0.0r
  Download and apply the upgrade from: http://ftp.openssl.org/source/openssl-1.0.0r.tar.gz
  Upgrade to version 1.0.0r of OpenSSL. The source code for this release can be downloaded from OpenSSL's website. To obtain binaries for your platform, please visit your vendor's site. Please note that many operating system vendors choose to apply the most recent OpenSSL security patches to their distributions without changing the package version to the most recent OpenSSL version

number.

- Upgrade to OpenSSL version 1.0.1m
  Download and apply the upgrade from: http://ftp.openssl.org/source/openssl-1.0.1m.tar.gz
  Upgrade to version 1.0.1m of OpenSSL. The source code for this release can be downloaded from OpenSSL's website. To obtain binaries for your platform, please visit your vendor's site. Please note that many operating system vendors choose to apply the most recent OpenSSL security patches to their distributions without changing the package version to the most recent OpenSSL version number.

- Upgrade to OpenSSL version 1.0.2a
  Download and apply the upgrade from: http://ftp.openssl.org/source/openssl-1.0.2a.tar.gz
  Upgrade to version 1.0.2a of OpenSSL. The source code for this release can be downloaded from OpenSSL's website. To obtain binaries for your platform, please visit your vendor's site. Please note that many operating system vendors choose to apply the most recent OpenSSL security patches to their distributions without changing the package version to the most recent OpenSSL version number.

3.2.45. Apache HTTPD: mod_dav crash (CVE-2013-1896) (apache-httpd-cve-2013-1896)

Description:

The affected asset is vulnerable to this vulnerability ONLY if it is running one of the following modules: mod_dav. Review your web server configuration for validation. Sending a MERGE request against a URI handled by mod_dav_svn with the source href (sent as part of the request body as XML) pointing to a URI that is not configured for DAV will trigger a segfault.

Affected Nodes:

Affected Nodes:	Additional Information:
xx.xxx.xx.xxx:80	• Running HTTP service • Product HTTPD exists -- Apache HTTPD 2.2.24 Vulnerable version of product HTTPD found -- Apache HTTPD 2.2.24
xx.xxx.xx.xxx:443	• Running HTTPS service • Product HTTPD exists -- Apache HTTPD 2.2.24 Vulnerable version of product HTTPD found -- Apache HTTPD 2.2.24

References:

Source	Reference
CVE	CVE-2013-1896
DISA_SEVERITY	Category I
DISA_VMSKEY	V0040288
IAVM	2013-A-0177
OVAL	OVAL18835
OVAL	OVAL19747
REDHAT	RHSA-2013:1156
REDHAT	RHSA-2013:1207
REDHAT	RHSA-2013:1208
REDHAT	RHSA-2013:1209

Source	Reference
URL	http://httpd.apache.org/security/vulnerabilities_22.html
URL	http://httpd.apache.org/security/vulnerabilities_24.html

Vulnerability Solution:

- Apache HTTPD >= 2.2 and < 2.2.25
  Upgrade to Apache HTTPD version 2.2.25
  Download and apply the upgrade from: http://archive.apache.org/dist/httpd/httpd-2.2.25.tar.gz
  Many platforms and distributions provide pre-built binary packages for Apache HTTP server. These pre-built packages are usually customized and optimized for a particular distribution, therefore we recommend that you use the packages if they are available for your operating system.

- Apache HTTPD >= 2.4 and < 2.4.6
  Upgrade to Apache HTTPD version 2.4.6
  Download and apply the upgrade from: http://archive.apache.org/dist/httpd/httpd-2.4.6.tar.gz
  Many platforms and distributions provide pre-built binary packages for Apache HTTP server. These pre-built packages are usually customized and optimized for a particular distribution, therefore we recommend that you use the packages if they are available for your operating system.

3.2.46. Apache HTTPD: mod_deflate denial of service (CVE-2014-0118) (apache-httpd-cve-2014-0118)

Description:

The affected asset is vulnerable to this vulnerability ONLY if it is running one of the following modules: mod_deflate. Review your web server configuration for validation. A resource consumption flaw was found in mod_deflate. If request body decompression was configured (using the "DEFLATE" input filter), a remote attacker could cause the server to consume significant memory and/or CPU resources. The use of request body decompression is not a common configuration.

Affected Nodes:

Affected Nodes:	Additional Information:
xx.xxx.xx.xxx:80	• Running HTTP service • Product HTTPD exists -- Apache HTTPD 2.2.24 Vulnerable version of product HTTPD found -- Apache HTTPD 2.2.24
xx.xxx.xx.xxx:443	• Running HTTPS service • Product HTTPD exists -- Apache HTTPD 2.2.24 Vulnerable version of product HTTPD found -- Apache HTTPD 2.2.24

References:

Source	Reference
APPLE	APPLE-SA-2015-04-08-2
BID	68745
CVE	CVE-2014-0118
DEBIAN	DSA-2989
DISA_SEVERITY	Category I
DISA_VMSKEY	V0053307
IAVM	2014-A-0114

Source	Reference
REDHAT	RHSA-2014:1019
REDHAT	RHSA-2014:1020
REDHAT	RHSA-2014:1021
URL	http://httpd.apache.org/security/vulnerabilities_22.html
URL	http://httpd.apache.org/security/vulnerabilities_24.html

Vulnerability Solution:

- Apache HTTPD >= 2.2 and < 2.2.29
  Upgrade to Apache HTTPD version 2.2.29
  Download and apply the upgrade from: http://archive.apache.org/dist/httpd/httpd-2.2.29.tar.gz
  Many platforms and distributions provide pre-built binary packages for Apache HTTP server. These pre-built packages are usually customized and optimized for a particular distribution, therefore we recommend that you use the packages if they are available for your operating system.

- Apache HTTPD >= 2.4 and < 2.4.10
  Upgrade to Apache HTTPD version 2.4.10
  Download and apply the upgrade from: http://archive.apache.org/dist/httpd/httpd-2.4.10.tar.gz
  Many platforms and distributions provide pre-built binary packages for Apache HTTP server. These pre-built packages are usually customized and optimized for a particular distribution, therefore we recommend that you use the packages if they are available for your operating system.

3.2.47. OpenSSL SSL_OP_NETSCAPE_REUSE_CIPHER_CHANGE_BUG ciphersuite downgrade (CVE-2010-4180) (http-openssl-cve-2010-4180)

Description:

OpenSSL before 0.9.8q, and 1.0.x before 1.0.0c, when SSL_OP_NETSCAPE_REUSE_CIPHER_CHANGE_BUG is enabled, does not properly prevent modification of the ciphersuite in the session cache, which allows remote attackers to force the downgrade to an unintended cipher via vectors involving sniffing network traffic to discover a session identifier.

Affected Nodes:

Affected Nodes:	Additional Information:
xx.xxx.xx.xxx:80	• Running HTTP service Vulnerable version of component OpenSSL found -- OpenSSL 1.0.0-fips
xx.xxx.xx.xxx:443	• Running HTTPS service Vulnerable version of component OpenSSL found -- OpenSSL 1.0.0-fips

References:

Source	Reference
APPLE	APPLE-SA-2011-06-23-1
BID	45164
CERT-VN	737740
CVE	CVE-2010-4180
DEBIAN	DSA-2141

Source	Reference
DISA_SEVERITY	Category I
DISA_VMSKEY	V0030769
DISA_VMSKEY	V0033794
DISA_VMSKEY	V0033884
IAVM	2011-A-0160
IAVM	2012-A-0148
IAVM	2012-A-0153
OSVDB	69565
OVAL	OVAL18910
REDHAT	RHSA-2010:0977
REDHAT	RHSA-2010:0978
REDHAT	RHSA-2010:0979
REDHAT	RHSA-2011:0896
URL	http://www.openssl.org/news/secadv_20101202.txt

Vulnerability Solution:

- Upgrade to OpenSSL version 0.9.8q
  Download and apply the upgrade from: http://ftp.openssl.org/source/openssl-0.9.8q.tar.gz
  Upgrade to version 0.9.8q of OpenSSL. The source code for this release can be downloaded from OpenSSL's website. To obtain binaries for your platform, please visit your vendor's site. Please note that many operating system vendors choose to apply the most recent OpenSSL security patches to their distributions without changing the package version to the most recent OpenSSL version number.

- Upgrade to OpenSSL version 1.0.0c
  Download and apply the upgrade from: http://ftp.openssl.org/source/openssl-1.0.0c.tar.gz
  Upgrade to version 1.0.0c of OpenSSL. The source code for this release can be downloaded from OpenSSL's website. To obtain binaries for your platform, please visit your vendor's site. Please note that many operating system vendors choose to apply the most recent OpenSSL security patches to their distributions without changing the package version to the most recent OpenSSL version number.

3.2.48. OpenSSL SSL_MODE_RELEASE_BUFFERS session injection or denial of service (CVE-2010-5298) (http-openssl-cve-2010-5298)

Description:

Race condition in the ssl3_read_bytes function in s3_pkt.c in OpenSSL through 1.0.1g, when SSL_MODE_RELEASE_BUFFERS is enabled, allows remote attackers to inject data across sessions or cause a denial of service (use-after-free and parsing error) via an SSL connection in a multithreaded environment.

Affected Nodes:

Affected Nodes:	Additional Information:
xx.xxx.xx.xxx:80	• Running HTTP service

Affected Nodes:	Additional Information:
	Vulnerable version of component OpenSSL found -- OpenSSL 1.0.0-fips
xx.xxx.xx.xxx:443	• Running HTTPS service Vulnerable version of component OpenSSL found -- OpenSSL 1.0.0-fips

References:

Source	Reference
BID	66801
CVE	CVE-2010-5298
DISA_SEVERITY	Category I
DISA_VMSKEY	V0052625
DISA_VMSKEY	V0052627
DISA_VMSKEY	V0052637
DISA_VMSKEY	V0052639
DISA_VMSKEY	V0052893
DISA_VMSKEY	V0052907
DISA_VMSKEY	V0052909
DISA_VMSKEY	V0052911
DISA_VMSKEY	V0053179
DISA_VMSKEY	V0053181
DISA_VMSKEY	V0053183
DISA_VMSKEY	V0053201
DISA_VMSKEY	V0053203
DISA_VMSKEY	V0053319
DISA_VMSKEY	V0053501
DISA_VMSKEY	V0053505
DISA_VMSKEY	V0053507
DISA_VMSKEY	V0053509
IAVM	2014-A-0087
IAVM	2014-A-0099
IAVM	2014-A-0100
IAVM	2014-A-0109
IAVM	2014-A-0110
IAVM	2014-A-0111

Source	Reference
IAVM	2014-A-0115
IAVM	2014-B-0077
IAVM	2014-B-0078
IAVM	2014-B-0080
IAVM	2014-B-0088
IAVM	2014-B-0089
IAVM	2014-B-0091
IAVM	2014-B-0092
IAVM	2014-B-0097
IAVM	2014-B-0101
IAVM	2014-B-0102
IAVM	2014-B-0103
URL	http://www.openssl.org/news/secadv_20140605.txt

Vulnerability Solution:

- Upgrade to OpenSSL version 1.0.0m
  Download and apply the upgrade from: http://ftp.openssl.org/source/openssl-1.0.0m.tar.gz
  Upgrade to version 1.0.0m of OpenSSL. The source code for this release can be downloaded from OpenSSL's website. To obtain binaries for your platform, please visit your vendor's site. Please note that many operating system vendors choose to apply the most recent OpenSSL security patches to their distributions without changing the package version to the most recent OpenSSL version number.

- Upgrade to OpenSSL version 1.0.1h
  Download and apply the upgrade from: http://ftp.openssl.org/source/openssl-1.0.1h.tar.gz
  Upgrade to version 1.0.1h of OpenSSL. The source code for this release can be downloaded from OpenSSL's website. To obtain binaries for your platform, please visit your vendor's site. Please note that many operating system vendors choose to apply the most recent OpenSSL security patches to their distributions without changing the package version to the most recent OpenSSL version number.

3.2.49. OpenSSL plaintext recovery attack against CBC mode encryption (CVE-2011-4108) (http-openssl-cve-2011-4108)

Description:

The DTLS implementation in OpenSSL before 0.9.8s and 1.x before 1.0.0f performs a MAC check only if certain padding is valid, which makes it easier for remote attackers to recover plaintext via a padding oracle attack.

Affected Nodes:

Affected Nodes:	Additional Information:
xx.xxx.xx.xxx:80	• Running HTTP service Vulnerable version of component OpenSSL found -- OpenSSL 1.0.0-fips
xx.xxx.xx.xxx:443	• Running HTTPS service Vulnerable version of component OpenSSL found -- OpenSSL 1.0.0-fips

References:

Source	Reference
APPLE	APPLE-SA-2013-06-04-1
CERT-VN	737740
CVE	CVE-2011-4108
DEBIAN	DSA-2390
DISA_SEVERITY	Category I
DISA_VMSKEY	V0033794
DISA_VMSKEY	V0033884
IAVM	2012-A-0148
IAVM	2012-A-0153
REDHAT	RHSA-2012:1306
REDHAT	RHSA-2012:1307
REDHAT	RHSA-2012:1308
URL	http://www.openssl.org/news/secadv_20120104.txt
URL	http://www.openssl.org/news/secadv_20120118.txt

Vulnerability Solution:

- Upgrade to OpenSSL version 0.9.8s
  Download and apply the upgrade from: http://ftp.openssl.org/source/openssl-0.9.8s.tar.gz
  Upgrade to version 0.9.8s of OpenSSL. The source code for this release can be downloaded from OpenSSL's website. To obtain binaries for your platform, please visit your vendor's site. Please note that many operating system vendors choose to apply the most recent OpenSSL security patches to their distributions without changing the package version to the most recent OpenSSL version number.

- Upgrade to OpenSSL version 1.0.0f
  Download and apply the upgrade from: http://ftp.openssl.org/source/openssl-1.0.0f.tar.gz
  Upgrade to version 1.0.0f of OpenSSL. The source code for this release can be downloaded from OpenSSL's website. To obtain binaries for your platform, please visit your vendor's site. Please note that many operating system vendors choose to apply the most recent OpenSSL security patches to their distributions without changing the package version to the most recent OpenSSL version number.

3.2.50. OpenSSL denial of service via malformed RFC 3779 data in certificates (CVE-2011-4577) (http-openssl-cve-2011-4577)

Description:

OpenSSL before 0.9.8s and 1.x before 1.0.0f, when RFC 3779 support is enabled, allows remote attackers to cause a denial of service (assertion failure) via an X.509 certificate containing certificate-extension data associated with (1) IP address blocks or (2) Autonomous System (AS) identifiers.

Affected Nodes:

Affected Nodes:	Additional Information:
xx.xxx.xx.xxx:80	• Running HTTP service Vulnerable version of component OpenSSL found -- OpenSSL 1.0.0-fips
xx.xxx.xx.xxx:443	• Running HTTPS service Vulnerable version of component OpenSSL found -- OpenSSL 1.0.0-fips

References:

Source	Reference
APPLE	APPLE-SA-2013-06-04-1
CERT-VN	737740
CVE	CVE-2011-4577
DISA_SEVERITY	Category I
DISA_VMSKEY	V0033794
DISA_VMSKEY	V0033884
IAVM	2012-A-0148
IAVM	2012-A-0153
URL	http://www.openssl.org/news/secadv_20120104.txt

Vulnerability Solution:

- Upgrade to OpenSSL version 0.9.8s
  Download and apply the upgrade from: http://ftp.openssl.org/source/openssl-0.9.8s.tar.gz
  Upgrade to version 0.9.8s of OpenSSL. The source code for this release can be downloaded from OpenSSL's website. To obtain binaries for your platform, please visit your vendor's site. Please note that many operating system vendors choose to apply the most recent OpenSSL security patches to their distributions without changing the package version to the most recent OpenSSL version number.

- Upgrade to OpenSSL version 1.0.0f
  Download and apply the upgrade from: http://ftp.openssl.org/source/openssl-1.0.0f.tar.gz
  Upgrade to version 1.0.0f of OpenSSL. The source code for this release can be downloaded from OpenSSL's website. To obtain binaries for your platform, please visit your vendor's site. Please note that many operating system vendors choose to apply the most recent OpenSSL security patches to their distributions without changing the package version to the most recent OpenSSL version number.

3.2.51. OpenSSL (CVE-2014-0076) (http-openssl-cve-2014-0076)

Description:

The Montgomery ladder implementation in OpenSSL through 1.0.0l does not ensure that certain swap operations have a constant-time behavior, which makes it easier for local users to obtain ECDSA nonces via a FLUSH+RELOAD cache side-channel attack.

Affected Nodes:

Affected Nodes:	Additional Information:
xx.xxx.xx.xxx:80	• Running HTTP service Vulnerable version of component OpenSSL found -- OpenSSL 1.0.0-fips

Affected Nodes:	Additional Information:
xx.xxx.xx.xxx:443	• Running HTTPS service Vulnerable version of component OpenSSL found -- OpenSSL 1.0.0-fips

References:

Source	Reference
BID	66363
CVE	CVE-2014-0076
DISA_SEVERITY	Category I
DISA_VMSKEY	V0052625
DISA_VMSKEY	V0052637
DISA_VMSKEY	V0053201
DISA_VMSKEY	V0053203
DISA_VMSKEY	V0054749
IAVM	2014-A-0087
IAVM	2014-A-0099
IAVM	2014-A-0100
IAVM	2014-A-0140
IAVM	2014-B-0077
URL	http://www.openssl.org/news/secadv_20140605.txt

Vulnerability Solution:

- Upgrade to OpenSSL version 0.9.8za
  Download and apply the upgrade from: http://ftp.openssl.org/source/openssl-0.9.8za.tar.gz
  Upgrade to version 0.9.8za of OpenSSL. The source code for this release can be downloaded from OpenSSL's website. To obtain binaries for your platform, please visit your vendor's site. Please note that many operating system vendors choose to apply the most recent OpenSSL security patches to their distributions without changing the package version to the most recent OpenSSL version number.

- Upgrade to OpenSSL version 1.0.0m
  Download and apply the upgrade from: http://ftp.openssl.org/source/openssl-1.0.0m.tar.gz
  Upgrade to version 1.0.0m of OpenSSL. The source code for this release can be downloaded from OpenSSL's website. To obtain binaries for your platform, please visit your vendor's site. Please note that many operating system vendors choose to apply the most recent OpenSSL security patches to their distributions without changing the package version to the most recent OpenSSL version number.

- Upgrade to OpenSSL version 1.0.1g
  Download and apply the upgrade from: http://ftp.openssl.org/source/openssl-1.0.1g.tar.gz
  Upgrade to version 1.0.1g of OpenSSL. The source code for this release can be downloaded from OpenSSL's website. To obtain binaries for your platform, please visit your vendor's site. Please note that many operating system vendors choose to apply the most recent OpenSSL security patches to their distributions without changing the package version to the most recent OpenSSL version number.

3.2.52. OpenSSL SSL_MODE_RELEASE_BUFFERS NULL pointer dereference (CVE-2014-0198) (http-openssl-cve-2014-0198)

Description:

The do_ssl3_write function in s3_pkt.c in OpenSSL 1.x through 1.0.1g, when SSL_MODE_RELEASE_BUFFERS is enabled, does not properly manage a buffer pointer during certain recursive calls, which allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via vectors that trigger an alert condition.

Affected Nodes:

Affected Nodes:	Additional Information:
xx.xxx.xx.xxx:80	• Running HTTP service Vulnerable version of component OpenSSL found -- OpenSSL 1.0.0-fips
xx.xxx.xx.xxx:443	• Running HTTPS service Vulnerable version of component OpenSSL found -- OpenSSL 1.0.0-fips

References:

Source	Reference
CVE	CVE-2014-0198
DEBIAN	DSA-2931
DISA_SEVERITY	Category I
DISA_VMSKEY	V0052625
DISA_VMSKEY	V0052627
DISA_VMSKEY	V0052637
DISA_VMSKEY	V0052639
DISA_VMSKEY	V0052641
DISA_VMSKEY	V0052893
DISA_VMSKEY	V0052907
DISA_VMSKEY	V0052909
DISA_VMSKEY	V0052911
DISA_VMSKEY	V0053179
DISA_VMSKEY	V0053181
DISA_VMSKEY	V0053183
DISA_VMSKEY	V0053201
DISA_VMSKEY	V0053203
DISA_VMSKEY	V0053319
DISA_VMSKEY	V0053501
DISA_VMSKEY	V0053505

Source	Reference
DISA_VMSKEY	V0053507
DISA_VMSKEY	V0053509
IAVM	2014-A-0087
IAVM	2014-A-0099
IAVM	2014-A-0100
IAVM	2014-A-0109
IAVM	2014-A-0110
IAVM	2014-A-0111
IAVM	2014-A-0115
IAVM	2014-B-0077
IAVM	2014-B-0078
IAVM	2014-B-0079
IAVM	2014-B-0080
IAVM	2014-B-0088
IAVM	2014-B-0089
IAVM	2014-B-0091
IAVM	2014-B-0092
IAVM	2014-B-0097
IAVM	2014-B-0101
IAVM	2014-B-0102
IAVM	2014-B-0103
URL	http://www.openssl.org/news/secadv_20140605.txt

Vulnerability Solution:

- Upgrade to OpenSSL version 1.0.0m
  Download and apply the upgrade from: http://ftp.openssl.org/source/openssl-1.0.0m.tar.gz
  Upgrade to version 1.0.0m of OpenSSL. The source code for this release can be downloaded from OpenSSL's website. To obtain binaries for your platform, please visit your vendor's site. Please note that many operating system vendors choose to apply the most recent OpenSSL security patches to their distributions without changing the package version to the most recent OpenSSL version number.

- Upgrade to OpenSSL version 1.0.1h
  Download and apply the upgrade from: http://ftp.openssl.org/source/openssl-1.0.1h.tar.gz
  Upgrade to version 1.0.1h of OpenSSL. The source code for this release can be downloaded from OpenSSL's website. To obtain binaries for your platform, please visit your vendor's site. Please note that many operating system vendors choose to apply the most recent OpenSSL security patches to their distributions without changing the package version to the most recent OpenSSL version number.

3.2.53. OpenSSL DTLS recursion flaw (CVE-2014-0221) (http-openssl-cve-2014-0221)

Description:

The dtls1_get_message_fragment function in d1_both.c in OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h allows remote attackers to cause a denial of service (recursion and client crash) via a DTLS hello message in an invalid DTLS handshake.

Affected Nodes:

Affected Nodes:	Additional Information:
xx.xxx.xx.xxx:80	• Running HTTP service Vulnerable version of component OpenSSL found -- OpenSSL 1.0.0-fips
xx.xxx.xx.xxx:443	• Running HTTPS service Vulnerable version of component OpenSSL found -- OpenSSL 1.0.0-fips

References:

Source	Reference
CVE	CVE-2014-0221
DISA_SEVERITY	Category I
DISA_VMSKEY	V0052625
DISA_VMSKEY	V0052627
DISA_VMSKEY	V0052637
DISA_VMSKEY	V0052641
DISA_VMSKEY	V0053201
DISA_VMSKEY	V0053203
DISA_VMSKEY	V0054749
IAVM	2014-A-0087
IAVM	2014-A-0099
IAVM	2014-A-0100
IAVM	2014-A-0140
IAVM	2014-B-0077
IAVM	2014-B-0079
IAVM	2014-B-0080
REDHAT	RHSA-2014:1021
URL	http://www.openssl.org/news/secadv_20140605.txt

Vulnerability Solution:

- Upgrade to OpenSSL version 0.9.8za
  Download and apply the upgrade from: http://ftp.openssl.org/source/openssl-0.9.8za.tar.gz
  Upgrade to version 0.9.8za of OpenSSL. The source code for this release can be downloaded from OpenSSL's website. To obtain

binaries for your platform, please visit your vendor's site. Please note that many operating system vendors choose to apply the most recent OpenSSL security patches to their distributions without changing the package version to the most recent OpenSSL version number.

- Upgrade to OpenSSL version 1.0.0m
  Download and apply the upgrade from: http://ftp.openssl.org/source/openssl-1.0.0m.tar.gz
  Upgrade to version 1.0.0m of OpenSSL. The source code for this release can be downloaded from OpenSSL's website. To obtain binaries for your platform, please visit your vendor's site. Please note that many operating system vendors choose to apply the most recent OpenSSL security patches to their distributions without changing the package version to the most recent OpenSSL version number.

- Upgrade to OpenSSL version 1.0.1h
  Download and apply the upgrade from: http://ftp.openssl.org/source/openssl-1.0.1h.tar.gz
  Upgrade to version 1.0.1h of OpenSSL. The source code for this release can be downloaded from OpenSSL's website. To obtain binaries for your platform, please visit your vendor's site. Please note that many operating system vendors choose to apply the most recent OpenSSL security patches to their distributions without changing the package version to the most recent OpenSSL version number.

3.2.54. OpenSSL Anonymous ECDH denial of service (CVE-2014-3470) (http-openssl-cve-2014-3470)

Description:

The ssl3_send_client_key_exchange function in s3_clnt.c in OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h, when an anonymous ECDH cipher suite is used, allows remote attackers to cause a denial of service (NULL pointer dereference and client crash) by triggering a NULL certificate value.

Affected Nodes:

Affected Nodes:	Additional Information:
xx.xxx.xx.xxx:80	• Running HTTP service Vulnerable version of component OpenSSL found -- OpenSSL 1.0.0-fips
xx.xxx.xx.xxx:443	• Running HTTPS service Vulnerable version of component OpenSSL found -- OpenSSL 1.0.0-fips

References:

Source	Reference
BID	67898
CVE	CVE-2014-3470
DISA_SEVERITY	Category I
DISA_VMSKEY	V0052625
DISA_VMSKEY	V0052627
DISA_VMSKEY	V0052637
DISA_VMSKEY	V0052641
DISA_VMSKEY	V0052893
DISA_VMSKEY	V0052907
DISA_VMSKEY	V0052909

Source	Reference
DISA_VMSKEY	V0052911
DISA_VMSKEY	V0053179
DISA_VMSKEY	V0053181
DISA_VMSKEY	V0053183
DISA_VMSKEY	V0053201
DISA_VMSKEY	V0053203
DISA_VMSKEY	V0053319
DISA_VMSKEY	V0053501
DISA_VMSKEY	V0053505
DISA_VMSKEY	V0053507
DISA_VMSKEY	V0053509
DISA_VMSKEY	V0054749
IAVM	2014-A-0087
IAVM	2014-A-0099
IAVM	2014-A-0100
IAVM	2014-A-0109
IAVM	2014-A-0110
IAVM	2014-A-0111
IAVM	2014-A-0115
IAVM	2014-A-0140
IAVM	2014-B-0077
IAVM	2014-B-0079
IAVM	2014-B-0080
IAVM	2014-B-0088
IAVM	2014-B-0089
IAVM	2014-B-0091
IAVM	2014-B-0092
IAVM	2014-B-0097
IAVM	2014-B-0101
IAVM	2014-B-0102
IAVM	2014-B-0103
URL	http://www.openssl.org/news/secadv_20140605.txt

Vulnerability Solution:

- Upgrade to OpenSSL version 0.9.8za
  Download and apply the upgrade from: http://ftp.openssl.org/source/openssl-0.9.8za.tar.gz
  Upgrade to version 0.9.8za of OpenSSL. The source code for this release can be downloaded from OpenSSL's website. To obtain binaries for your platform, please visit your vendor's site. Please note that many operating system vendors choose to apply the most recent OpenSSL security patches to their distributions without changing the package version to the most recent OpenSSL version number.

- Upgrade to OpenSSL version 1.0.0m
  Download and apply the upgrade from: http://ftp.openssl.org/source/openssl-1.0.0m.tar.gz
  Upgrade to version 1.0.0m of OpenSSL. The source code for this release can be downloaded from OpenSSL's website. To obtain binaries for your platform, please visit your vendor's site. Please note that many operating system vendors choose to apply the most recent OpenSSL security patches to their distributions without changing the package version to the most recent OpenSSL version number.

- Upgrade to OpenSSL version 1.0.1h
  Download and apply the upgrade from: http://ftp.openssl.org/source/openssl-1.0.1h.tar.gz
  Upgrade to version 1.0.1h of OpenSSL. The source code for this release can be downloaded from OpenSSL's website. To obtain binaries for your platform, please visit your vendor's site. Please note that many operating system vendors choose to apply the most recent OpenSSL security patches to their distributions without changing the package version to the most recent OpenSSL version number.

3.2.55. OpenSSL (CVE-2014-3508) (http-openssl-cve-2014-3508)

Description:

The OBJ_obj2txt function in crypto/objects/obj_dat.c in OpenSSL 0.9.8 before 0.9.8zb, 1.0.0 before 1.0.0n, and 1.0.1 before 1.0.1i, when pretty printing is used, does not ensure the presence of '\0' characters, which allows context-dependent attackers to obtain sensitive information from process stack memory by reading output from X509_name_oneline, X509_name_print_ex, and unspecified other functions.

Affected Nodes:

Affected Nodes:	Additional Information:
xx.xxx.xx.xxx:80	• Running HTTP service Vulnerable version of component OpenSSL found -- OpenSSL 1.0.0-fips
xx.xxx.xx.xxx:443	• Running HTTPS service Vulnerable version of component OpenSSL found -- OpenSSL 1.0.0-fips

References:

Source	Reference
CVE	CVE-2014-3508
DEBIAN	DSA-2998
DISA_SEVERITY	Category I
DISA_VMSKEY	V0053793
IAVM	2014-A-0122
NETBSD	NetBSD-SA2014-008

Source	Reference
REDHAT	RHSA-2014:1256
REDHAT	RHSA-2014:1297
URL	http://www.openssl.org/news/secadv_20140806.txt

Vulnerability Solution:

- Upgrade to OpenSSL version 0.9.8zb
  Download and apply the upgrade from: http://ftp.openssl.org/source/openssl-0.9.8zb.tar.gz
  Upgrade to version 0.9.8zb of OpenSSL. The source code for this release can be downloaded from OpenSSL's website. To obtain binaries for your platform, please visit your vendor's site. Please note that many operating system vendors choose to apply the most recent OpenSSL security patches to their distributions without changing the package version to the most recent OpenSSL version number.

- Upgrade to OpenSSL version 1.0.0n
  Download and apply the upgrade from: http://ftp.openssl.org/source/openssl-1.0.0n.tar.gz
  Upgrade to version 1.0.0n of OpenSSL. The source code for this release can be downloaded from OpenSSL's website. To obtain binaries for your platform, please visit your vendor's site. Please note that many operating system vendors choose to apply the most recent OpenSSL security patches to their distributions without changing the package version to the most recent OpenSSL version number.

- Upgrade to OpenSSL version 1.0.1i
  Download and apply the upgrade from: http://ftp.openssl.org/source/openssl-1.0.1i.tar.gz
  Upgrade to version 1.0.1i of OpenSSL. The source code for this release can be downloaded from OpenSSL's website. To obtain binaries for your platform, please visit your vendor's site. Please note that many operating system vendors choose to apply the most recent OpenSSL security patches to their distributions without changing the package version to the most recent OpenSSL version number.

3.2.56. OpenSSL (CVE-2014-3510) (http-openssl-cve-2014-3510)

Description:

The ssl3_send_client_key_exchange function in s3_clnt.c in OpenSSL 0.9.8 before 0.9.8zb, 1.0.0 before 1.0.0n, and 1.0.1 before 1.0.1i allows remote DTLS servers to cause a denial of service (NULL pointer dereference and client application crash) via a crafted handshake message in conjunction with a (1) anonymous DH or (2) anonymous ECDH ciphersuite.

Affected Nodes:

Affected Nodes:	Additional Information:
xx.xxx.xx.xxx:80	• Running HTTP service Vulnerable version of component OpenSSL found -- OpenSSL 1.0.0-fips
xx.xxx.xx.xxx:443	• Running HTTPS service Vulnerable version of component OpenSSL found -- OpenSSL 1.0.0-fips

References:

Source	Reference
BID	69082
CVE	CVE-2014-3510
DEBIAN	DSA-2998

Source	Reference
DISA_SEVERITY	Category I
DISA_VMSKEY	V0053793
IAVM	2014-A-0122
NETBSD	NetBSD-SA2014-008
REDHAT	RHSA-2014:1256
REDHAT	RHSA-2014:1297
URL	http://www.openssl.org/news/secadv_20140806.txt

Vulnerability Solution:

- Upgrade to OpenSSL version 0.9.8zb
  Download and apply the upgrade from: http://ftp.openssl.org/source/openssl-0.9.8zb.tar.gz
  Upgrade to version 0.9.8zb of OpenSSL. The source code for this release can be downloaded from OpenSSL's website. To obtain binaries for your platform, please visit your vendor's site. Please note that many operating system vendors choose to apply the most recent OpenSSL security patches to their distributions without changing the package version to the most recent OpenSSL version number.

- Upgrade to OpenSSL version 1.0.0n
  Download and apply the upgrade from: http://ftp.openssl.org/source/openssl-1.0.0n.tar.gz
  Upgrade to version 1.0.0n of OpenSSL. The source code for this release can be downloaded from OpenSSL's website. To obtain binaries for your platform, please visit your vendor's site. Please note that many operating system vendors choose to apply the most recent OpenSSL security patches to their distributions without changing the package version to the most recent OpenSSL version number.

- Upgrade to OpenSSL version 1.0.1i
  Download and apply the upgrade from: http://ftp.openssl.org/source/openssl-1.0.1i.tar.gz
  Upgrade to version 1.0.1i of OpenSSL. The source code for this release can be downloaded from OpenSSL's website. To obtain binaries for your platform, please visit your vendor's site. Please note that many operating system vendors choose to apply the most recent OpenSSL security patches to their distributions without changing the package version to the most recent OpenSSL version number.

3.2.57. OpenSSL SSL 3.0 Fallback protection (CVE-2014-3566) (http-openssl-cve-2014-3566)

Description:

The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.

Affected Nodes:

Affected Nodes:	Additional Information:
xx.xxx.xx.xxx:80	• Running HTTP service Vulnerable version of component OpenSSL found -- OpenSSL 1.0.0-fips
xx.xxx.xx.xxx:443	• Running HTTPS service Vulnerable version of component OpenSSL found -- OpenSSL 1.0.0-fips

References:

Source	Reference

Source	Reference
APPLE	APPLE-SA-2014-10-16-1
APPLE	APPLE-SA-2014-10-16-3
APPLE	APPLE-SA-2014-10-16-4
APPLE	APPLE-SA-2014-10-20-1
APPLE	APPLE-SA-2014-10-20-2
APPLE	APPLE-SA-2015-01-27-4
BID	70574
CERT	TA14-290A
CERT-VN	577193
CVE	CVE-2014-3566
DEBIAN	DSA-3053
DEBIAN	DSA-3144
DEBIAN	DSA-3147
DEBIAN	DSA-3253
NETBSD	NetBSD-SA2014-015
REDHAT	RHSA-2014:1652
REDHAT	RHSA-2014:1653
REDHAT	RHSA-2014:1692
REDHAT	RHSA-2014:1876
REDHAT	RHSA-2014:1877
REDHAT	RHSA-2014:1880
REDHAT	RHSA-2014:1881
REDHAT	RHSA-2014:1882
REDHAT	RHSA-2014:1920
REDHAT	RHSA-2014:1948
REDHAT	RHSA-2015:0068
REDHAT	RHSA-2015:0079
REDHAT	RHSA-2015:0080
REDHAT	RHSA-2015:0085
REDHAT	RHSA-2015:0086
REDHAT	RHSA-2015:0264
REDHAT	RHSA-2015:0698

Source	Reference
URL	http://www.openssl.org/news/secadv_20141015.txt

Vulnerability Solution:

- Upgrade to OpenSSL version 0.9.8zc
  Download and apply the upgrade from: http://ftp.openssl.org/source/openssl-0.9.8zc.tar.gz
  Upgrade to version 0.9.8zc of OpenSSL. The source code for this release can be downloaded from OpenSSL's website. To obtain binaries for your platform, please visit your vendor's site. Please note that many operating system vendors choose to apply the most recent OpenSSL security patches to their distributions without changing the package version to the most recent OpenSSL version number.

- Upgrade to OpenSSL version 1.0.0o
  Download and apply the upgrade from: http://ftp.openssl.org/source/openssl-1.0.0o.tar.gz
  Upgrade to version 1.0.0o of OpenSSL. The source code for this release can be downloaded from OpenSSL's website. To obtain binaries for your platform, please visit your vendor's site. Please note that many operating system vendors choose to apply the most recent OpenSSL security patches to their distributions without changing the package version to the most recent OpenSSL version number.

- Upgrade to OpenSSL version 1.0.1j
  Download and apply the upgrade from: http://ftp.openssl.org/source/openssl-1.0.1j.tar.gz
  Upgrade to version 1.0.1j of OpenSSL. The source code for this release can be downloaded from OpenSSL's website. To obtain binaries for your platform, please visit your vendor's site. Please note that many operating system vendors choose to apply the most recent OpenSSL security patches to their distributions without changing the package version to the most recent OpenSSL version number.

3.2.58. OpenSSL (CVE-2014-3568) (http-openssl-cve-2014-3568)

Description:

OpenSSL before 0.9.8zc, 1.0.0 before 1.0.0o, and 1.0.1 before 1.0.1j does not properly enforce the no-ssl3 build option, which allows remote attackers to bypass intended access restrictions via an SSL 3.0 handshake, related to s23_clnt.c and s23_srvr.c.

Affected Nodes:

Affected Nodes:	Additional Information:
xx.xxx.xx.xxx:80	• Running HTTP service Vulnerable version of component OpenSSL found -- OpenSSL 1.0.0-fips
xx.xxx.xx.xxx:443	• Running HTTPS service Vulnerable version of component OpenSSL found -- OpenSSL 1.0.0-fips

References:

Source	Reference
APPLE	APPLE-SA-2015-01-27-4
BID	70585
CVE	CVE-2014-3568
DEBIAN	DSA-3053
NETBSD	NetBSD-SA2014-015
URL	http://www.openssl.org/news/secadv_20141015.txt

Source	Reference
XF	97037

Vulnerability Solution:

- Upgrade to OpenSSL version 0.9.8zc
  Download and apply the upgrade from: http://ftp.openssl.org/source/openssl-0.9.8zc.tar.gz
  Upgrade to version 0.9.8zc of OpenSSL. The source code for this release can be downloaded from OpenSSL's website. To obtain binaries for your platform, please visit your vendor's site. Please note that many operating system vendors choose to apply the most recent OpenSSL security patches to their distributions without changing the package version to the most recent OpenSSL version number.

- Upgrade to OpenSSL version 1.0.0o
  Download and apply the upgrade from: http://ftp.openssl.org/source/openssl-1.0.0o.tar.gz
  Upgrade to version 1.0.0o of OpenSSL. The source code for this release can be downloaded from OpenSSL's website. To obtain binaries for your platform, please visit your vendor's site. Please note that many operating system vendors choose to apply the most recent OpenSSL security patches to their distributions without changing the package version to the most recent OpenSSL version number.

- Upgrade to OpenSSL version 1.0.1j
  Download and apply the upgrade from: http://ftp.openssl.org/source/openssl-1.0.1j.tar.gz
  Upgrade to version 1.0.1j of OpenSSL. The source code for this release can be downloaded from OpenSSL's website. To obtain binaries for your platform, please visit your vendor's site. Please note that many operating system vendors choose to apply the most recent OpenSSL security patches to their distributions without changing the package version to the most recent OpenSSL version number.

3.2.59. OpenSSL (CVE-2014-8176) (http-openssl-cve-2014-8176)

Description:

The dtls1_clear_queues function in ssl/d1_lib.c in OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h frees data structures without considering that application data can arrive between a ChangeCipherSpec message and a Finished message, which allows remote DTLS peers to cause a denial of service (memory corruption and application crash) or possibly have unspecified other impact via unexpected application data.

Affected Nodes:

Affected Nodes:	Additional Information:
xx.xxx.xx.xxx:80	• Running HTTP service Vulnerable version of component OpenSSL found -- OpenSSL 1.0.0-fips
xx.xxx.xx.xxx:443	• Running HTTPS service Vulnerable version of component OpenSSL found -- OpenSSL 1.0.0-fips

References:

Source	Reference
CVE	CVE-2014-8176
URL	http://www.openssl.org/news/secadv_20150611.txt

Vulnerability Solution:

- Upgrade to OpenSSL version 0.9.8za
  Download and apply the upgrade from: http://ftp.openssl.org/source/openssl-0.9.8za.tar.gz
  Upgrade to version 0.9.8za of OpenSSL. The source code for this release can be downloaded from OpenSSL's website. To obtain

binaries for your platform, please visit your vendor's site. Please note that many operating system vendors choose to apply the most recent OpenSSL security patches to their distributions without changing the package version to the most recent OpenSSL version number.

- Upgrade to OpenSSL version 1.0.0m
  Download and apply the upgrade from: http://ftp.openssl.org/source/openssl-1.0.0m.tar.gz
  Upgrade to version 1.0.0m of OpenSSL. The source code for this release can be downloaded from OpenSSL's website. To obtain binaries for your platform, please visit your vendor's site. Please note that many operating system vendors choose to apply the most recent OpenSSL security patches to their distributions without changing the package version to the most recent OpenSSL version number.

- Upgrade to OpenSSL version 1.0.1h
  Download and apply the upgrade from: http://ftp.openssl.org/source/openssl-1.0.1h.tar.gz
  Upgrade to version 1.0.1h of OpenSSL. The source code for this release can be downloaded from OpenSSL's website. To obtain binaries for your platform, please visit your vendor's site. Please note that many operating system vendors choose to apply the most recent OpenSSL security patches to their distributions without changing the package version to the most recent OpenSSL version number.

3.2.60. OpenSSL (CVE-2015-0204) (http-openssl-cve-2015-0204)

Description:

The ssl3_get_key_exchange function in s3_clnt.c in OpenSSL before 0.9.8zd, 1.0.0 before 1.0.0p, and 1.0.1 before 1.0.1k allows remote SSL servers to conduct RSA-to-EXPORT_RSA downgrade attacks and facilitate brute-force decryption by offering a weak ephemeral RSA key in a noncompliant role, related to the "FREAK" issue. NOTE: the scope of this CVE is only client code based on OpenSSL, not EXPORT_RSA issues associated with servers or other TLS implementations.

Affected Nodes:

Affected Nodes:	Additional Information:
xx.xxx.xx.xxx:80	• Running HTTP service Vulnerable version of component OpenSSL found -- OpenSSL 1.0.0-fips
xx.xxx.xx.xxx:443	• Running HTTPS service Vulnerable version of component OpenSSL found -- OpenSSL 1.0.0-fips

References:

Source	Reference
APPLE	APPLE-SA-2015-04-08-2
CVE	CVE-2015-0204
DEBIAN	DSA-3125
REDHAT	RHSA-2015:0066
REDHAT	RHSA-2015:0800
REDHAT	RHSA-2015:0849
URL	http://www.openssl.org/news/secadv_20150108.txt
URL	http://www.openssl.org/news/secadv_20150319.txt

Vulnerability Solution:

- Upgrade to OpenSSL version 0.9.8zd
  Download and apply the upgrade from: http://ftp.openssl.org/source/openssl-0.9.8zd.tar.gz
  Upgrade to version 0.9.8zd of OpenSSL. The source code for this release can be downloaded from OpenSSL's website. To obtain binaries for your platform, please visit your vendor's site. Please note that many operating system vendors choose to apply the most recent OpenSSL security patches to their distributions without changing the package version to the most recent OpenSSL version number.

- Upgrade to OpenSSL version 1.0.0p
  Download and apply the upgrade from: http://ftp.openssl.org/source/openssl-1.0.0p.tar.gz
  Upgrade to version 1.0.0p of OpenSSL. The source code for this release can be downloaded from OpenSSL's website. To obtain binaries for your platform, please visit your vendor's site. Please note that many operating system vendors choose to apply the most recent OpenSSL security patches to their distributions without changing the package version to the most recent OpenSSL version number.

- Upgrade to OpenSSL version 1.0.1k
  Download and apply the upgrade from: http://ftp.openssl.org/source/openssl-1.0.1k.tar.gz
  Upgrade to version 1.0.1k of OpenSSL. The source code for this release can be downloaded from OpenSSL's website. To obtain binaries for your platform, please visit your vendor's site. Please note that many operating system vendors choose to apply the most recent OpenSSL security patches to their distributions without changing the package version to the most recent OpenSSL version number.

3.2.61. OpenSSL (CVE-2015-1788) (http-openssl-cve-2015-1788)

Description:

The BN_GF2m_mod_inv function in crypto/bn/bn_gf2m.c in OpenSSL before 0.9.8s, 1.0.0 before 1.0.0e, 1.0.1 before 1.0.1n, and 1.0.2 before 1.0.2b does not properly handle ECParameters structures in which the curve is over a malformed binary polynomial field, which allows remote attackers to cause a denial of service (infinite loop) via a session that uses an Elliptic Curve algorithm, as demonstrated by an attack against a server that supports client authentication.

Affected Nodes:

Affected Nodes:	Additional Information:
xx.xxx.xx.xxx:80	• Running HTTP service Vulnerable version of component OpenSSL found -- OpenSSL 1.0.0-fips
xx.xxx.xx.xxx:443	• Running HTTPS service Vulnerable version of component OpenSSL found -- OpenSSL 1.0.0-fips

References:

Source	Reference
CVE	CVE-2015-1788
URL	http://www.openssl.org/news/secadv_20150611.txt

Vulnerability Solution:

- Upgrade to OpenSSL version 0.9.8s
  Download and apply the upgrade from: http://ftp.openssl.org/source/openssl-0.9.8s.tar.gz
  Upgrade to version 0.9.8s of OpenSSL. The source code for this release can be downloaded from OpenSSL's website. To obtain binaries for your platform, please visit your vendor's site. Please note that many operating system vendors choose to apply the most recent OpenSSL security patches to their distributions without changing the package version to the most recent OpenSSL version number.

- Upgrade to OpenSSL version 1.0.0e

Download and apply the upgrade from: http://ftp.openssl.org/source/openssl-1.0.0e.tar.gz
Upgrade to version 1.0.0e of OpenSSL. The source code for this release can be downloaded from OpenSSL's website. To obtain binaries for your platform, please visit your vendor's site. Please note that many operating system vendors choose to apply the most recent OpenSSL security patches to their distributions without changing the package version to the most recent OpenSSL version number.

- Upgrade to OpenSSL version 1.0.1n
  Download and apply the upgrade from: http://ftp.openssl.org/source/openssl-1.0.1n.tar.gz
  Upgrade to version 1.0.1n of OpenSSL. The source code for this release can be downloaded from OpenSSL's website. To obtain binaries for your platform, please visit your vendor's site. Please note that many operating system vendors choose to apply the most recent OpenSSL security patches to their distributions without changing the package version to the most recent OpenSSL version number.

- Upgrade to OpenSSL version 1.0.2b
  Download and apply the upgrade from: http://ftp.openssl.org/source/openssl-1.0.2b.tar.gz
  Upgrade to version 1.0.2b of OpenSSL. The source code for this release can be downloaded from OpenSSL's website. To obtain binaries for your platform, please visit your vendor's site. Please note that many operating system vendors choose to apply the most recent OpenSSL security patches to their distributions without changing the package version to the most recent OpenSSL version number.

3.2.62. OpenSSL (CVE-2015-1789) (http-openssl-cve-2015-1789)

Description:

The X509_cmp_time function in crypto/x509/x509_vfy.c in OpenSSL before 0.9.8zg, 1.0.0 before 1.0.0s, 1.0.1 before 1.0.1n, and 1.0.2 before 1.0.2b allows remote attackers to cause a denial of service (out-of-bounds read and application crash) via a crafted length field in ASN1_TIME data, as demonstrated by an attack against a server that supports client authentication with a custom verification callback.

Affected Nodes:

Affected Nodes:	Additional Information:
xx.xxx.xx.xxx:80	• Running HTTP service Vulnerable version of component OpenSSL found -- OpenSSL 1.0.0-fips
xx.xxx.xx.xxx:443	• Running HTTPS service Vulnerable version of component OpenSSL found -- OpenSSL 1.0.0-fips

References:

Source	Reference
CVE	CVE-2015-1789
URL	http://www.openssl.org/news/secadv_20150611.txt

Vulnerability Solution:

- Upgrade to OpenSSL version 0.9.8zg
  Download and apply the upgrade from: http://ftp.openssl.org/source/openssl-0.9.8zg.tar.gz
  Upgrade to version 0.9.8zg of OpenSSL. The source code for this release can be downloaded from OpenSSL's website. To obtain binaries for your platform, please visit your vendor's site. Please note that many operating system vendors choose to apply the most recent OpenSSL security patches to their distributions without changing the package version to the most recent OpenSSL version number.

- Upgrade to OpenSSL version 1.0.0s
  Download and apply the upgrade from: http://ftp.openssl.org/source/openssl-1.0.0s.tar.gz

Upgrade to version 1.0.0s of OpenSSL. The source code for this release can be downloaded from OpenSSL's website. To obtain binaries for your platform, please visit your vendor's site. Please note that many operating system vendors choose to apply the most recent OpenSSL security patches to their distributions without changing the package version to the most recent OpenSSL version number.

- Upgrade to OpenSSL version 1.0.1n
  Download and apply the upgrade from: http://ftp.openssl.org/source/openssl-1.0.1n.tar.gz
  Upgrade to version 1.0.1n of OpenSSL. The source code for this release can be downloaded from OpenSSL's website. To obtain binaries for your platform, please visit your vendor's site. Please note that many operating system vendors choose to apply the most recent OpenSSL security patches to their distributions without changing the package version to the most recent OpenSSL version number.

- Upgrade to OpenSSL version 1.0.2b
  Download and apply the upgrade from: http://ftp.openssl.org/source/openssl-1.0.2b.tar.gz
  Upgrade to version 1.0.2b of OpenSSL. The source code for this release can be downloaded from OpenSSL's website. To obtain binaries for your platform, please visit your vendor's site. Please note that many operating system vendors choose to apply the most recent OpenSSL security patches to their distributions without changing the package version to the most recent OpenSSL version number.

3.2.63. OpenSSL (CVE-2015-1790) (http-openssl-cve-2015-1790)

Description:

The PKCS7_dataDecodefunction in crypto/pkcs7/pk7_doit.c in OpenSSL before 0.9.8zg, 1.0.0 before 1.0.0s, 1.0.1 before 1.0.1n, and 1.0.2 before 1.0.2b allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a PKCS#7 blob that uses ASN.1 encoding and lacks inner EncryptedContent data.

Affected Nodes:

Affected Nodes:	Additional Information:
xx.xxx.xx.xxx:80	• Running HTTP service Vulnerable version of component OpenSSL found -- OpenSSL 1.0.0-fips
xx.xxx.xx.xxx:443	• Running HTTPS service Vulnerable version of component OpenSSL found -- OpenSSL 1.0.0-fips

References:

Source	Reference
CVE	CVE-2015-1790
URL	http://www.openssl.org/news/secadv_20150611.txt

Vulnerability Solution:

- Upgrade to OpenSSL version 0.9.8zg
  Download and apply the upgrade from: http://ftp.openssl.org/source/openssl-0.9.8zg.tar.gz
  Upgrade to version 0.9.8zg of OpenSSL. The source code for this release can be downloaded from OpenSSL's website. To obtain binaries for your platform, please visit your vendor's site. Please note that many operating system vendors choose to apply the most recent OpenSSL security patches to their distributions without changing the package version to the most recent OpenSSL version number.

- Upgrade to OpenSSL version 1.0.0s
  Download and apply the upgrade from: http://ftp.openssl.org/source/openssl-1.0.0s.tar.gz
  Upgrade to version 1.0.0s of OpenSSL. The source code for this release can be downloaded from OpenSSL's website. To obtain binaries for your platform, please visit your vendor's site. Please note that many operating system vendors choose to apply the most

recent OpenSSL security patches to their distributions without changing the package version to the most recent OpenSSL version number.

- Upgrade to OpenSSL version 1.0.1n
  Download and apply the upgrade from: http://ftp.openssl.org/source/openssl-1.0.1n.tar.gz
  Upgrade to version 1.0.1n of OpenSSL. The source code for this release can be downloaded from OpenSSL's website. To obtain binaries for your platform, please visit your vendor's site. Please note that many operating system vendors choose to apply the most recent OpenSSL security patches to their distributions without changing the package version to the most recent OpenSSL version number.

- Upgrade to OpenSSL version 1.0.2b
  Download and apply the upgrade from: http://ftp.openssl.org/source/openssl-1.0.2b.tar.gz
  Upgrade to version 1.0.2b of OpenSSL. The source code for this release can be downloaded from OpenSSL's website. To obtain binaries for your platform, please visit your vendor's site. Please note that many operating system vendors choose to apply the most recent OpenSSL security patches to their distributions without changing the package version to the most recent OpenSSL version number.

3.2.64. OpenSSL (CVE-2015-1791) (http-openssl-cve-2015-1791)

Description:

Race condition in the ssl3_get_new_session_ticket function in ssl/s3_clnt.c in OpenSSL before 0.9.8zg, 1.0.0 before 1.0.0s, 1.0.1 before 1.0.1n, and 1.0.2 before 1.0.2b, when used for a multi-threaded client, allows remote attackers to cause a denial of service (double free and application crash) or possibly have unspecified other impact by providing a NewSessionTicket during an attempt to reuse a ticket that had been obtained earlier.

Affected Nodes:

Affected Nodes:	Additional Information:
xx.xxx.xx.xxx:80	• Running HTTP service Vulnerable version of component OpenSSL found -- OpenSSL 1.0.0-fips
xx.xxx.xx.xxx:443	• Running HTTPS service Vulnerable version of component OpenSSL found -- OpenSSL 1.0.0-fips

References:

Source	Reference
CVE	CVE-2015-1791
URL	http://www.openssl.org/news/secadv_20150611.txt

Vulnerability Solution:

- Upgrade to OpenSSL version 0.9.8zg
  Download and apply the upgrade from: http://ftp.openssl.org/source/openssl-0.9.8zg.tar.gz
  Upgrade to version 0.9.8zg of OpenSSL. The source code for this release can be downloaded from OpenSSL's website. To obtain binaries for your platform, please visit your vendor's site. Please note that many operating system vendors choose to apply the most recent OpenSSL security patches to their distributions without changing the package version to the most recent OpenSSL version number.

- Upgrade to OpenSSL version 1.0.0s
  Download and apply the upgrade from: http://ftp.openssl.org/source/openssl-1.0.0s.tar.gz
  Upgrade to version 1.0.0s of OpenSSL. The source code for this release can be downloaded from OpenSSL's website. To obtain binaries for your platform, please visit your vendor's site. Please note that many operating system vendors choose to apply the most recent OpenSSL security patches to their distributions without changing the package version to the most recent OpenSSL version

number.

- Upgrade to OpenSSL version 1.0.1n
  Download and apply the upgrade from: http://ftp.openssl.org/source/openssl-1.0.1n.tar.gz
  Upgrade to version 1.0.1n of OpenSSL. The source code for this release can be downloaded from OpenSSL's website. To obtain binaries for your platform, please visit your vendor's site. Please note that many operating system vendors choose to apply the most recent OpenSSL security patches to their distributions without changing the package version to the most recent OpenSSL version number.

- Upgrade to OpenSSL version 1.0.2b
  Download and apply the upgrade from: http://ftp.openssl.org/source/openssl-1.0.2b.tar.gz
  Upgrade to version 1.0.2b of OpenSSL. The source code for this release can be downloaded from OpenSSL's website. To obtain binaries for your platform, please visit your vendor's site. Please note that many operating system vendors choose to apply the most recent OpenSSL security patches to their distributions without changing the package version to the most recent OpenSSL version number.

3.2.65. OpenSSL (CVE-2015-1792) (http-openssl-cve-2015-1792)

Description:

The do_free_upto function in crypto/cms/cms_smime.c in OpenSSL before 0.9.8zg, 1.0.0 before 1.0.0s, 1.0.1 before 1.0.1n, and 1.0.2 before 1.0.2b allows remote attackers to cause a denial of service (infinite loop) via vectors that trigger a NULL value of a BIO data structure, as demonstrated by an unrecognized X.660 OID for a hash function.

Affected Nodes:

Affected Nodes:	Additional Information:
xx.xxx.xx.xxx:80	• Running HTTP service Vulnerable version of component OpenSSL found -- OpenSSL 1.0.0-fips
xx.xxx.xx.xxx:443	• Running HTTPS service Vulnerable version of component OpenSSL found -- OpenSSL 1.0.0-fips

References:

Source	Reference
CVE	CVE-2015-1792
URL	http://www.openssl.org/news/secadv_20150611.txt

Vulnerability Solution:

- Upgrade to OpenSSL version 0.9.8zg
  Download and apply the upgrade from: http://ftp.openssl.org/source/openssl-0.9.8zg.tar.gz
  Upgrade to version 0.9.8zg of OpenSSL. The source code for this release can be downloaded from OpenSSL's website. To obtain binaries for your platform, please visit your vendor's site. Please note that many operating system vendors choose to apply the most recent OpenSSL security patches to their distributions without changing the package version to the most recent OpenSSL version number.

- Upgrade to OpenSSL version 1.0.0s
  Download and apply the upgrade from: http://ftp.openssl.org/source/openssl-1.0.0s.tar.gz
  Upgrade to version 1.0.0s of OpenSSL. The source code for this release can be downloaded from OpenSSL's website. To obtain binaries for your platform, please visit your vendor's site. Please note that many operating system vendors choose to apply the most recent OpenSSL security patches to their distributions without changing the package version to the most recent OpenSSL version number.

- Upgrade to OpenSSL version 1.0.1n
  Download and apply the upgrade from: http://ftp.openssl.org/source/openssl-1.0.1n.tar.gz
  Upgrade to version 1.0.1n of OpenSSL. The source code for this release can be downloaded from OpenSSL's website. To obtain binaries for your platform, please visit your vendor's site. Please note that many operating system vendors choose to apply the most recent OpenSSL security patches to their distributions without changing the package version to the most recent OpenSSL version number.

- Upgrade to OpenSSL version 1.0.2b
  Download and apply the upgrade from: http://ftp.openssl.org/source/openssl-1.0.2b.tar.gz
  Upgrade to version 1.0.2b of OpenSSL. The source code for this release can be downloaded from OpenSSL's website. To obtain binaries for your platform, please visit your vendor's site. Please note that many operating system vendors choose to apply the most recent OpenSSL security patches to their distributions without changing the package version to the most recent OpenSSL version number.

3.2.66. OpenSSL SSL 3.0 Fallback protection (CVE-2014-3566) (openssl-openssl-cve-2014-3566)

Description:

The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.

Affected Nodes:

Affected Nodes:	Additional Information:
xx.xxx.xx.xxx:80	• Running HTTP service Vulnerable version of component OpenSSL found -- OpenSSL 1.0.0-fips
xx.xxx.xx.xxx:443	• Running HTTPS service Vulnerable version of component OpenSSL found -- OpenSSL 1.0.0-fips

References:

Source	Reference
APPLE	APPLE-SA-2014-10-16-1
APPLE	APPLE-SA-2014-10-16-3
APPLE	APPLE-SA-2014-10-16-4
APPLE	APPLE-SA-2014-10-20-1
APPLE	APPLE-SA-2014-10-20-2
APPLE	APPLE-SA-2015-01-27-4
BID	70574
CERT	TA14-290A
CERT-VN	577193
CVE	CVE-2014-3566
DEBIAN	DSA-3053
DEBIAN	DSA-3144

Source	Reference
DEBIAN	DSA-3147
DEBIAN	DSA-3253
NETBSD	NetBSD-SA2014-015
REDHAT	RHSA-2014:1652
REDHAT	RHSA-2014:1653
REDHAT	RHSA-2014:1692
REDHAT	RHSA-2014:1876
REDHAT	RHSA-2014:1877
REDHAT	RHSA-2014:1880
REDHAT	RHSA-2014:1881
REDHAT	RHSA-2014:1882
REDHAT	RHSA-2014:1920
REDHAT	RHSA-2014:1948
REDHAT	RHSA-2015:0068
REDHAT	RHSA-2015:0079
REDHAT	RHSA-2015:0080
REDHAT	RHSA-2015:0085
REDHAT	RHSA-2015:0086
REDHAT	RHSA-2015:0264
REDHAT	RHSA-2015:0698
URL	http://www.openssl.org/news/secadv_20141015.txt

Vulnerability Solution:

- Upgrade to OpenSSL version 0.9.8zc
  Download and apply the upgrade from: http://ftp.openssl.org/source/openssl-0.9.8zc.tar.gz
  Upgrade to version 0.9.8zc of OpenSSL. The source code for this release can be downloaded from OpenSSL's website. To obtain binaries for your platform, please visit your vendor's site. Please note that many operating system vendors choose to apply the most recent OpenSSL security patches to their distributions without changing the package version to the most recent OpenSSL version number.

- Upgrade to OpenSSL version 1.0.0o
  Download and apply the upgrade from: http://ftp.openssl.org/source/openssl-1.0.0o.tar.gz
  Upgrade to version 1.0.0o of OpenSSL. The source code for this release can be downloaded from OpenSSL's website. To obtain binaries for your platform, please visit your vendor's site. Please note that many operating system vendors choose to apply the most recent OpenSSL security patches to their distributions without changing the package version to the most recent OpenSSL version number.

- Upgrade to OpenSSL version 1.0.1j
  Download and apply the upgrade from: http://ftp.openssl.org/source/openssl-1.0.1j.tar.gz
  Upgrade to version 1.0.1j of OpenSSL. The source code for this release can be downloaded from OpenSSL's website. To obtain

binaries for your platform, please visit your vendor's site. Please note that many operating system vendors choose to apply the most recent OpenSSL security patches to their distributions without changing the package version to the most recent OpenSSL version number.

3.3. Moderate Vulnerabilities

3.3.1. ISC BIND: A Crafted Query Against an NSEC3-signed Zone Can Crash BIND (CVE-2014-0591) (dns-bind-cve-2014-0591)

Description:

The query_findclosestnsec3 function in query.c in named in ISC BIND 9.6, 9.7, and 9.8 before 9.8.6-P2 and 9.9 before 9.9.4-P2, and 9.6-ESV before 9.6-ESV-R10-P2, allows remote attackers to cause a denial of service (INSIST assertion failure and daemon exit) via a crafted DNS query to an authoritative nameserver that uses the NSEC3 signing feature.

Affected Nodes:

Affected Nodes:	Additional Information:
xx.xxx.xx.xxx:53	• Running DNS service • Product BIND exists -- BIND 9.8.2rc1-RedHat-9.8.2-0.23.rc1.el6_5.1 Vulnerable version of product BIND found -- BIND 9.8.2rc1-RedHat-9.8.2-0.23.rc1.el6_5.1

References:

Source	Reference
APPLE	APPLE-SA-2014-10-16-3
BID	64801
CVE	CVE-2014-0591
DEBIAN	DSA-3023
DISA_SEVERITY	Category I
DISA_VMSKEY	V0052635
IAVM	2014-A-0086
OSVDB	101973
REDHAT	RHSA-2014:0043
URL	https://kb.isc.org/article/AA-01078/0
URL	https://kb.isc.org/article/AA-01078/74/CVE-2014-0591%3A-A-Crafted-Query-Against-an-NSEC3-signed-Zone-Can-Crash-BIND.html

Vulnerability Solution:

More information about upgrading your version of ISC BIND is available on the ISC website.

3.3.2. OpenSSL (CVE-2013-0169) (http-openssl-cve-2013-0169)

Description:

The TLS protocol 1.1 and 1.2 and the DTLS protocol 1.0 and 1.2, as used in OpenSSL, OpenJDK, PolarSSL, and other products, do not properly consider timing side-channel attacks on a MAC check requirement during the processing of malformed CBC padding, which allows remote attackers to conduct distinguishing attacks and plaintext-recovery attacks via statistical analysis of timing data for crafted packets, aka the "Lucky Thirteen" issue.

Affected Nodes:

Affected Nodes:	Additional Information:
xx.xxx.xx.xxx:80	• Running HTTP service Vulnerable version of component OpenSSL found -- OpenSSL 1.0.0-fips
xx.xxx.xx.xxx:443	• Running HTTPS service Vulnerable version of component OpenSSL found -- OpenSSL 1.0.0-fips

References:

Source	Reference
APPLE	APPLE-SA-2013-09-12-1
CERT	TA13-051A
CERT-VN	737740
CVE	CVE-2013-0169
DEBIAN	DSA-2621
DEBIAN	DSA-2622
OVAL	OVAL18841
OVAL	OVAL19016
OVAL	OVAL19424
OVAL	OVAL19540
OVAL	OVAL19608
REDHAT	RHSA-2013:0587
REDHAT	RHSA-2013:0782
REDHAT	RHSA-2013:0783
REDHAT	RHSA-2013:0833
REDHAT	RHSA-2013:1455
REDHAT	RHSA-2013:1456
URL	http://www.openssl.org/news/secadv_20130205.txt

Vulnerability Solution:

- Upgrade to OpenSSL version 0.9.8y
  Download and apply the upgrade from: http://ftp.openssl.org/source/openssl-0.9.8y.tar.gz
  Upgrade to version 0.9.8y of OpenSSL. The source code for this release can be downloaded from OpenSSL's website. To obtain binaries for your platform, please visit your vendor's site. Please note that many operating system vendors choose to apply the most recent OpenSSL security patches to their distributions without changing the package version to the most recent OpenSSL version number.

- Upgrade to OpenSSL version 1.0.0k
  Download and apply the upgrade from: http://ftp.openssl.org/source/openssl-1.0.0k.tar.gz
  Upgrade to version 1.0.0k of OpenSSL. The source code for this release can be downloaded from OpenSSL's website. To obtain binaries for your platform, please visit your vendor's site. Please note that many operating system vendors choose to apply the most recent OpenSSL security patches to their distributions without changing the package version to the most recent OpenSSL version number.

- Upgrade to OpenSSL version 1.0.1d
  Download and apply the upgrade from: http://ftp.openssl.org/source/openssl-1.0.1d.tar.gz
  Upgrade to version 1.0.1d of OpenSSL. The source code for this release can be downloaded from OpenSSL's website. To obtain binaries for your platform, please visit your vendor's site. Please note that many operating system vendors choose to apply the most recent OpenSSL security patches to their distributions without changing the package version to the most recent OpenSSL version number.

4. Discovered Services

4.1. DNS

4.1.1. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
xx.xxx.xx.xxx	tcp	53	5	• BIND 9.8.2rc1-RedHat-9.8.2-0.23.rc1.el6_5.1 bind.version: 9.8.2rc1-RedHat-9.8.2-0.23.rc1.el6_5.1

4.2. FTP

4.2.1. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
xx.xxx.xx.xxx	tcp	21	1	• ftp.plaintext.authentication: true ftp.supports-starttls: true

4.3. HTTP

4.3.1. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
xx.xxx.xx.xxx	tcp	80	6	• Apache HTTPD 2.2.24 • FrontPage: 5.0.2.2635 • OpenSSL: 1.0.0-fips • http.banner: Apache/2.2.24 (Unix) mod_ssl/2.2.24 OpenSSL/1.0.0-fips mod_auth_passthrough/2.1 mod_bwlimited/1.4 FrontPage/5.0.2.2635 mod_perl/2.0.6 Perl/v5.10.1 • http.banner.server: Apache/2.2.24 (Unix) mod_ssl/2.2.24 OpenSSL/1.0.0-fips mod_auth_passthrough/2.1 mod_bwlimited/1.4 FrontPage/5.0.2.2635 mod_perl/2.0.6 Perl/v5.10.1 • mod_ssl: 2.2.24 • verbs-1: GET • verbs-2: HEAD • verbs-3: OPTIONS • verbs-4: POST • verbs-5: TRACE verbs-count: 5

4.4. HTTPS

4.4.1. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information

Device	Protocol	Port	Vulnerabilities	Additional Information
xx.xxx.xx.xxx	tcp	443	6	• Apache HTTPD 2.2.24 • FrontPage: 5.0.2.2635 • OpenSSL: 1.0.0-fips • http.banner: Apache/2.2.24 (Unix) mod_ssl/2.2.24 OpenSSL/1.0.0-fips mod_auth_passthrough/2.1 mod_bwlimited/1.4 FrontPage/5.0.2.2635 mod_perl/2.0.6 Perl/v5.10.1 • http.banner.server: Apache/2.2.24 (Unix) mod_ssl/2.2.24 OpenSSL/1.0.0-fips mod_auth_passthrough/2.1 mod_bwlimited/1.4 FrontPage/5.0.2.2635 mod_perl/2.0.6 Perl/v5.10.1 • mod_ssl: 2.2.24 • ssl: true • SAMPLE • ssl.cert.version: 3 • verbs-1: GET • verbs-2: HEAD • verbs-3: OPTIONS • verbs-4: POST • verbs-5: TRACE verbs-count: 5

4.5. IMAP

4.5.1. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
xx.xxx.xx.xxx	tcp	143	0	

4.6. IMAPS

4.6.1. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
xx.xxx.xx.xxx	tcp	993	1	• Dovecot • imap.banner: * OK [CAPABILITY IMAP4rev1 LITERAL+ SASL-IR LOGIN-REFERRALS ID ENABLE IDLE NAMESPACE AUTH=PLAIN AUTH=LOGIN] Dovecot ready. SAMPLE ONLY

4.7. MySQL

4.7.1. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
xx.xxx.xx.xxx	tcp	3306	1	

4.8. POP

4.8.1. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
xx.xxx.xx.xxx	tcp	110	0	

4.9. POPS

4.9.1. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
xx.xxx.xx.xxx	tcp	995	1	• Dovecot • pop.banner: +OK Dovecot ready. • pop.plaintext.authentication: true • ssl: true • ssl.cert.chainerror: basic constraints check failed: pathLenConstraint violated - this cert must be the last cert in the certification path • SAMPLE • ssl.cert.sig.alg.name: SHA256withRSA • SAMPLE • ssl.cert.validchain: false ssl.cert.version: 3

4.10. SMTP

4.10.1. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
xx.xxx.xx.xxx	tcp	587	2	• advertised-esmtp-extension-count: 6 • advertises-esmtp: TRUE • max-message-size: 52428800 • smtp.plaintext.authentication: true • SAMPLE • supports-pipelining: TRUE • supports-size: TRUE • supports-starttls: TRUE • supports-turn: FALSE supports-verify: FALSE

4.11. SSH

4.11.1. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
xx.xxx.xx.xxx	tcp	22	0	

5. Discovered Users and Groups

No user or group information was discovered during the scan.

6. Discovered Databases

No database information was discovered during the scan.

7. Discovered Files and Directories

No file or directory information was discovered during the scan.

8. Policy Evaluations

No policy evaluations were performed.

9. Spidered Web Sites

No web sites were spidered during the scan.