CVE-2015-3194

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2015-3194
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-12-06 20:59:00 UTC
Updated	2023-11-07 02:25:00 UTC
Description	crypto/rsa/rsa_ameth.c in OpenSSL 1.0.1 before 1.0.1q and 1.0.2 before 1.0.2e allows remote attackers to cause a denial c

Risk And Classification

Problem Types: CWE-476

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	12.04	All	All	All
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	15.04	All	All	All
Operating System	Canonical	Ubuntu Linux	15.10	All	All	All
Operating System	Canonical	Ubuntu Linux	12.04	All	All	All
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	15.04	All	All	All
Operating System	Canonical	Ubuntu Linux	15.10	All	All	All
Operating System	Debian	Debian Linux	7.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	7.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Application	Nodejs	Node.js	All	All	All	All
Application	Nodejs	Node.js	All	All	All	All
Application	Openssl	Openssl	1.0.1	All	All	All
Application	Openssl	Openssl	1.0.1a	All	All	All
Application	Openssl	Openssl	1.0.1b	All	All	All

Application	Openssl	Openssl	1.0.1c	All	All	All
Application	Openssl	Openssl	1.0.1d	All	All	All
Application	Openssl	Openssl	1.0.1e	All	All	All
Application	Openssl	Openssl	1.0.1f	All	All	All
Application	Openssl	Openssl	1.0.1g	All	All	All
Application	Openssl	Openssl	1.0.1h	All	All	All
Application	Openssl	Openssl	1.0.1i	All	All	All
Application	Openssl	Openssl	1.0.1j	All	All	All
Application	Openssl	Openssl	1.0.1k	All	All	All
Application	Openssl	Openssl	1.0.1l	All	All	All
Application	Openssl	Openssl	1.0.1m	All	All	All
Application	Openssl	Openssl	1.0.1n	All	All	All
Application	Openssl	Openssl	1.0.1o	All	All	All
Application	Openssl	Openssl	1.0.1p	All	All	All
Application	Openssl	Openssl	1.0.2	All	All	All
Application	Openssl	Openssl	1.0.2a	All	All	All
Application	Openssl	Openssl	1.0.2b	All	All	All
Application	Openssl	Openssl	1.0.2c	All	All	All
Application	Openssl	Openssl	1.0.2d	All	All	All
Application	Openssl	Openssl	1.0.1	All	All	All
Application	Openssl	Openssl	1.0.1a	All	All	All
Application	Openssl	Openssl	1.0.1b	All	All	All
Application	Openssl	Openssl	1.0.1c	All	All	All
Application	Openssl	Openssl	1.0.1d	All	All	All
Application	Openssl	Openssl	1.0.1e	All	All	All
Application	Openssl	Openssl	1.0.1f	All	All	All
Application	Openssl	Openssl	1.0.1g	All	All	All
Application	Openssl	Openssl	1.0.1h	All	All	All
Application	Openssl	Openssl	1.0.1i	All	All	All
Application	Openssl	Openssl	1.0.1j	All	All	All
Application	Openssl	Openssl	1.0.1k	All	All	All
Application	Openssl	Openssl	1.0.1l	All	All	All
Application	Openssl	Openssl	1.0.1m	All	All	All
Application	Openssl	Openssl	1.0.1n	All	All	All
Application	Openssl	Openssl	1.0.1o	All	All	All

Application	Openssl	Openssl	1.0.1p	All	All	All
Application	Openssl	Openssl	1.0.2	All	All	All
Application	Openssl	Openssl	1.0.2a	All	All	All
Application	Openssl	Openssl	1.0.2b	All	All	All
Application	Openssl	Openssl	1.0.2c	All	All	All
Application	Openssl	Openssl	1.0.2d	All	All	All

References

Reference	Source	Li
Oracle Critical Patch Update Advisory - April 2016	CONFIRM	ww
USN-2830-1: OpenSSL vulnerabilities | Ubuntu	UBUNTU	ww
Multiple Vulnerabilities in OpenSSL (December 2015) Affecting Cisco Products	CISCO	toc
[security-announce] openSUSE-SU-2016:0637-1: important: Security update	SUSE	list
Oracle Critical Patch Update - July 2016	CONFIRM	ww
Bug 1288320 – CVE-2015-3194 OpenSSL: Certificate verify crash with missing PSS parameter	CONFIRM	bu
openssl.org/news/secadv/20151203.txt	CONFIRM	op
HPE Support document - HPE Support Center	CONFIRM	h2
Oracle July 2016 Critical Patch Update Multiple Vulnerabilities	BID	ww
Debian -- Security Information -- DSA-3413-1 openssl	DEBIAN	ww
Red Hat Customer Portal	REDHAT	rhr
FortiGuard.com | OpenSSL Advisory - December 2015	CONFIRM	for
openSUSE-SU-2015:2288-1: moderate: Security update for OpenSSL	SUSE	list
Document Display | HPE Support Center	CONFIRM	h2
[SECURITY] Fedora 22 Update: openssl-1.0.1k-13.fc22	FEDORA	list
Document Display | HPE Support Center	CONFIRM	h2
openSUSE-SU-2015:2289-1: moderate: Security update for openssl	SUSE	list
Document Display | HPE Support Center	CONFIRM	h2
Public KB - SA40100 - [Pulse Secure] December 3rd 2015 OpenSSL Security Advisory	CONFIRM	kb
git.openssl.org Git - openssl.git/commit		git
2016-10 Security Bulletin: CTPView: Multiple vulnerabilities in CTPView - Juniper Networks	CONFIRM	kb
OpenSSL CVE-2015-3194 Denial of Service Vulnerability	BID	ww
git.openssl.org Git - openssl.git/commit	CONFIRM	git
'[security bulletin] HPSBGN03536 rev.1 - HP IceWall Products running OpenSSL, Remote and Local Denial' - MARC	HP	ma
Oracle Linux Bulletin - October 2015	CONFIRM	ww
cert-portal.siemens.com/productcert/pdf/ssa-412672.pdf	CONFIRM	ce
Document Display | HPE Support Center	CONFIRM	h2

git.openssl.org Git - openssl.git/commit		git
Document Display | HPE Support Center	CONFIRM	h2
FortiGuard.com | OpenSSL Advisory - December 2015	CONFIRM	ww
Juniper Networks - 2016-10 Security Bulletin: OpenSSL security updates	CONFIRM	kb
OpenSSL Multiple Bugs Let Remote Users Deny Service and Obtain Potentially Sensitive Information - SecurityTracker	SECTRACK	ww
Document Display | HPE Support Center	CONFIRM	h2
openSUSE-SU-2015:2318-1: moderate: Security update for libressl	SUSE	list
The Slackware Linux Project: Slackware Security Advisories	SLACKWARE	ww
git.openssl.org Git - openssl.git/commit	CONFIRM	git
[security-announce] openSUSE-SU-2016:1332-1: important: Security update	SUSE	list
Oracle Critical Patch Update - October 2017	CONFIRM	ww
Red Hat Customer Portal	REDHAT	rhr
Oracle Solaris Bulletin - January 2016	CONFIRM	ww
CVE Program record	CVE.ORG	ww
NVD vulnerability detail	NVD	nv

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

375442 HPE System Management Homepage Multiple Vulnerabilities (HPESBMU03593)

390226 Oracle Managed Virtualization (VM) Server for x86 Security Update for Open Secure Sockets Layer (OpenSSL) (OVMSA-2021-0011)

390284 Oracle Managed Virtualization (VM) Server for x86 Security Update for Open Secure Sockets Layer (OpenSSL) (OVMSA-2023-0013)

591280 Siemens SCALANCE X-200RNA Switch Devices Denial of Service (DoS) Multiple Vulnerabilities (ICSA-22-349-21, SSA-412672)