CVE-2016-0702

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2016-0702
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2016-03-03 20:59:00 UTC
Updated	2023-11-07 02:29:00 UTC
Description	The MOD_EXP_CTIME_COPY_FROM_PREBUF function in crypto/bn/bn_exp.c in OpenSSL 1.0.1 before 1.0.1s and 1.0.2

Risk And Classification

Problem Types: CWE-200

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	15.10	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	Nodejs	Node.js	All	All	All	All
Application	Openssl	Openssl	1.0.1	All	All	All
Application	Openssl	Openssl	1.0.1	beta1	All	All
Application	Openssl	Openssl	1.0.1	beta2	All	All
Application	Openssl	Openssl	1.0.1	beta3	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	1.0.1q	All	All	All
Application	Openssl	Openssl	1.0.1r	All	All	All
Application	Openssl	Openssl	1.0.2	All	All	All
Application	Openssl	Openssl	1.0.2	beta1	All	All
Application	Openssl	Openssl	1.0.2	beta2	All	All
Application	Openssl	Openssl	1.0.2	beta3	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	1.0.2e	All	All	All
Application	Openssl	Openssl	1.0.2f	All	All	All
Application	Openssl	Openssl	1.0.1	All	All	All
Application	Openssl	Openssl	1.0.1	beta1	All	All
Application	Openssl	Openssl	1.0.1	beta2	All	All
Application	Openssl	Openssl	1.0.1	beta3	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	1.0.1q	All	All	All
Application	Openssl	Openssl	1.0.1r	All	All	All
Application	Openssl	Openssl	1.0.2	All	All	All
Application	Openssl	Openssl	1.0.2	beta1	All	All
Application	Openssl	Openssl	1.0.2	beta2	All	All
Application	Openssl	Openssl	1.0.2	beta3	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	1.0.2e	All	All	All
Application	Openssl	Openssl	1.0.2f	All	All	All

References

Reference	Source	Link
[security-announce] openSUSE-SU-2016:1566-1: important: Security update	SUSE	lists.ope
Oracle Solaris Bulletin - April 2016	CONFIRM	www.or
Oracle Critical Patch Update Advisory - April 2016	CONFIRM	www.or
'[security bulletin] HPSBGN03563 rev.1 - HPE IceWall Products using OpenSSL, Remote Denial of Service' - MARC	HP	marc.in
[security-announce] openSUSE-SU-2016:0637-1: important: Security update	SUSE	lists.ope
[security-announce] openSUSE-SU-2016:1273-1: important: Security update	SUSE	lists.ope
[security-announce] SUSE-SU-2016:0617-1: important: Security update for	SUSE	lists.ope
git.openssl.org Git - openssl.git/commit	CONFIRM	git.oper
[security-announce] SUSE-SU-2016:1360-1: important: Security update for	SUSE	lists.ope
[security-announce] openSUSE-SU-2016:0720-1: important: Security update	SUSE	lists.ope
[security-announce] openSUSE-SU-2016:0627-1: important: Security update	SUSE	lists.ope
[security-announce] SUSE-SU-2016:0624-1: important: Security update for	SUSE	lists.ope
[security-announce] SUSE-SU-2016:0620-1: important: Security update for	SUSE	lists.ope

OpenSSL Flaws Let Remote Users Deny Service and Decrypt TLS Sessions in Certain Cases - SecurityTracker	SECTRACK	www.se
OpenSSL: Multiple vulnerabilities (GLSA 201603-15) — Gentoo Security	GENTOO	security
HPE Support document - HPE Support Center	CONFIRM	h20566
[security-announce] openSUSE-SU-2016:1242-1: important: Security update	SUSE	lists.ope
www.openssl.org/news/secadv/20160301.txt	CONFIRM	www.op
[security-announce] SUSE-SU-2016:1057-1: important: Security update for	SUSE	lists.ope
Document Display | HPE Support Center	CONFIRM	h20566
Multiple Vulnerabilities in OpenSSL Affecting Cisco Products: March 2016	CISCO	tools.cis
[security-announce] SUSE-SU-2016:1290-1: important: Security update for	SUSE	lists.ope
[security-announce] openSUSE-SU-2016:0638-1: important: Security update	SUSE	lists.ope
openssl.org/news/secadv/20160301.txt	CONFIRM	openssl
[security-announce] openSUSE-SU-2016:0628-1: important: Security update	SUSE	lists.ope
[security-announce] SUSE-SU-2016:0631-1: important: Security update for	SUSE	lists.ope
CacheBleed: A Timing Attack on OpenSSL Constant Time RSA	MISC	cachebl
[security-announce] openSUSE-SU-2016:1241-1: important: Security update	SUSE	lists.ope
[security-announce] SUSE-SU-2016:0641-1: important: Security update for	SUSE	lists.ope
[security-announce] SUSE-SU-2016:1267-1: important: Security update for	SUSE	lists.ope
cert-portal.siemens.com/productcert/pdf/ssa-412672.pdf	CONFIRM	cert-por
git.openssl.org Git - openssl.git/commit		git.oper
Oracle Linux Bulletin - January 2016	CONFIRM	www.or
FreeBSD-SA-16:12	FREEBSD	security
Debian -- Security Information -- DSA-3500-1 openssl	DEBIAN	www.de
[security-announce] SUSE-SU-2016:0621-1: important: Security update for	SUSE	lists.ope
USN-2914-1: OpenSSL vulnerabilities | Ubuntu	UBUNTU	www.ub
Juniper Networks - 2016-10 Security Bulletin: OpenSSL security updates	CONFIRM	kb.junip
Public KB - SA40168 - [Pulse Secure] March 1st 2016 OpenSSL Security Advisory	CONFIRM	kb.pulse
Document Display | HPE Support Center	CONFIRM	h20566
[SECURITY] Fedora 22 Update: openssl-1.0.1k-14.fc22	FEDORA	lists.fed
[security-announce] openSUSE-SU-2016:1239-1: important: Security update	SUSE	lists.ope
Document Display | HPE Support Center	CONFIRM	h20566
Red Hat Customer Portal	REDHAT	rhn.redh
[SECURITY] Fedora 23 Update: openssl-1.0.2g-2.fc23	FEDORA	lists.fed
CVE Program record	CVE.ORG	www.cv
NVD vulnerability detail	NVD	nvd.nist

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

- 378509 Splunk Enterprise Multiple Vulnerabilities (SP-CAAAPKV)
- 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)
- 591311 Bosch Rexroth PRA-ES8P2S Ethernet-Switch Multiple Vulnerabilities (BOSCH-SA-247053-BT)