CVE-2016-0798

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2016-0798
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2016-03-03 20:59:00 UTC
Updated	2023-02-12 23:16:00 UTC
Description	Memory leak in the SRP_VBASE_get_by_user implementation in OpenSSL 1.0.1 before 1.0.1s and 1.0.2 before 1.0.2g allo

Risk And Classification

Problem Types: CWE-399

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
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
Oracle Solaris Bulletin - April 2016	CONFIRM	www.oracle
Oracle Critical Patch Update Advisory - April 2016	CONFIRM	www.oracle
git.openssl.org Git - openssl.git/commit	CONFIRM	git.openssl.(
[security-announce] openSUSE-SU-2016:0637-1: important: Security update	SUSE	lists.opensu
[security-announce] SUSE-SU-2016:0617-1: important: Security update for	SUSE	lists.opensu
Oracle Critical Patch Update - July 2016	CONFIRM	www.oracle
[security-announce] openSUSE-SU-2016:0627-1: important: Security update	SUSE	lists.opensu
[security-announce] SUSE-SU-2016:0620-1: important: Security update for	SUSE	lists.opensu
Oracle July 2016 Critical Patch Update Multiple Vulnerabilities	BID	www.securi
OpenSSL CVE-2016-0798 Memory Leak Denial of Service Vulnerability	BID	www.securi
OpenSSL Flaws Let Remote Users Deny Service and Decrypt TLS Sessions in Certain Cases - SecurityTracker	SECTRACK	www.securi
OpenSSL: Multiple vulnerabilities (GLSA 201603-15) — Gentoo Security	GENTOO	security.ger
HPE Support document - HPE Support Center	CONFIRM	h20566.ww
www.openssl.org/news/secadv/20160301.txt	CONFIRM	www.opens
git.openssl.org Git - openssl.git/commit	MISC	git.openssl.(
Multiple Vulnerabilities in OpenSSL Affecting Cisco Products: March 2016	CISCO	tools.cisco.(
[security-announce] openSUSE-SU-2016:0638-1: important: Security update	SUSE	lists.opensu
openssl.org/news/secadv/20160301.txt	CONFIRM	openssl.org
[security-announce] openSUSE-SU-2016:0628-1: important: Security update	SUSE	lists.opensu
cert-portal.siemens.com/productcert/pdf/ssa-412672.pdf	CONFIRM	cert-portal.s
FreeBSD-SA-16:12	FREEBSD	security.Fre

Debian -- Security Information -- DSA-3500-1 openssl	DEBIAN	www.debian
[security-announce] SUSE-SU-2016:0621-1: important: Security update for	SUSE	lists.opensu
USN-2914-1: OpenSSL vulnerabilities | Ubuntu	UBUNTU	www.ubuntu
Juniper Networks - 2016-10 Security Bulletin: OpenSSL security updates	CONFIRM	kb.juniper.n
Public KB - SA40168 - [Pulse Secure] March 1st 2016 OpenSSL Security Advisory	CONFIRM	kb.pulsesec
CVE Program record	CVE.ORG	www.cve.or
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

378509 Splunk Enterprise Multiple Vulnerabilities (SP-CAAAPKV)

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)