



CVE-2016-0798

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

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 allc

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.com
Oracle Critical Patch Update Advisory - April 2016	CONFIRM	www.oracle.com
git.openssl.org Git - openssl.git/commit	CONFIRM	git.openssl.org
[security-announce] openSUSE-SU-2016:0637-1: important: Security update	SUSE	lists.opensuse.org
[security-announce] SUSE-SU-2016:0617-1: important: Security update for	SUSE	lists.opensuse.org
Oracle Critical Patch Update - July 2016	CONFIRM	www.oracle.com
[security-announce] openSUSE-SU-2016:0627-1: important: Security update	SUSE	lists.opensuse.org
[security-announce] SUSE-SU-2016:0620-1: important: Security update for	SUSE	lists.opensuse.org
Oracle July 2016 Critical Patch Update Multiple Vulnerabilities	BID	www.securityfocus.com
OpenSSL CVE-2016-0798 Memory Leak Denial of Service Vulnerability	BID	www.securityfocus.com
OpenSSL Flaws Let Remote Users Deny Service and Decrypt TLS Sessions in Certain Cases - SecurityTracker	SECTRACK	www.securityfocus.com
OpenSSL: Multiple vulnerabilities (GLSA 201603-15) — Gentoo Security	GENTOO	security.gentoo.org
HPE Support document - HPE Support Center	CONFIRM	h20566.www2.hp.com
www.openssl.org/news/secadv/20160301.txt	CONFIRM	www.openssl.org
git.openssl.org Git - openssl.git/commit	MISC	git.openssl.org
Multiple Vulnerabilities in OpenSSL Affecting Cisco Products: March 2016	CISCO	tools.cisco.com
[security-announce] openSUSE-SU-2016:0638-1: important: Security update	SUSE	lists.opensuse.org
openssl.org/news/secadv/20160301.txt	CONFIRM	openssl.org
[security-announce] openSUSE-SU-2016:0628-1: important: Security update	SUSE	lists.opensuse.org
cert-portal.siemens.com/productcert/pdf/ssa-412672.pdf	CONFIRM	cert-portal.siemens.com
FreeBSD-SA-16:12	FREEBSD	security.FreeBSD.org

Debian -- Security Information -- DSA-3500-1 openssl	DEBIAN	www.debian.org
[security-announce] SUSE-SU-2016:0621-1: important: Security update for	SUSE	lists.opensuse.org
USN-2914-1: OpenSSL vulnerabilities Ubuntu	UBUNTU	www.ubuntu.com
Juniper Networks - 2016-10 Security Bulletin: OpenSSL security updates	CONFIRM	kb.juniper.net
Public KB - SA40168 - [Pulse Secure] March 1st 2016 OpenSSL Security Advisory	CONFIRM	kb.pulsesecure.net
CVE Program record	CVE.ORG	www.cve.org
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)

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)