



# CVE-2016-0797

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

## Summary

<b>CVE</b>	CVE-2016-0797
<b>State</b>	PUBLIC
<b>Assigner</b>	secalert@redhat.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2016-03-03 20:59:00 UTC
<b>Updated</b>	2023-11-07 02:29:00 UTC
<b>Description</b>	Multiple integer overflows in OpenSSL 1.0.1 before 1.0.1s and 1.0.2 before 1.0.2g allow remote attackers to cause a denial

## Risk And Classification

**Problem Types:** NVD-CWE-Other

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	12.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	14.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	15.10	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	7.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	8.0	All	All	All
Application	<a href="#">Nodejs</a>	<a href="#">Node.js</a>	All	All	All	All
Application	<a href="#">Nodejs</a>	<a href="#">Node.js</a>	All	All	All	All
Application	<a href="#">Nodejs</a>	<a href="#">Node.js</a>	All	All	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	1.0.1	All	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	1.0.1	beta1	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	1.0.1	beta2	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	1.0.1	beta3	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	1.0.1a	All	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	1.0.1b	All	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	1.0.1c	All	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	1.0.1d	All	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	1.0.1e	All	All	All

Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	1.0.1f	All	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	1.0.1g	All	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	1.0.1h	All	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	1.0.1i	All	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	1.0.1j	All	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	1.0.1k	All	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	1.0.1l	All	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	1.0.1m	All	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	1.0.1n	All	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	1.0.1o	All	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	1.0.1p	All	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	1.0.1q	All	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	1.0.1r	All	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	1.0.2	All	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	1.0.2	beta1	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	1.0.2	beta2	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	1.0.2	beta3	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	1.0.2a	All	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	1.0.2b	All	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	1.0.2c	All	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	1.0.2d	All	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	1.0.2e	All	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	1.0.2f	All	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	1.0.1	All	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	1.0.1	beta1	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	1.0.1	beta2	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	1.0.1	beta3	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	1.0.1a	All	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	1.0.1b	All	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	1.0.1c	All	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	1.0.1d	All	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	1.0.1e	All	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	1.0.1f	All	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	1.0.1g	All	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	1.0.1h	All	All	All

Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	1.0.1i	All	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	1.0.1j	All	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	1.0.1k	All	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	1.0.1l	All	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	1.0.1m	All	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	1.0.1n	All	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	1.0.1o	All	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	1.0.1p	All	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	1.0.1q	All	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	1.0.1r	All	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	1.0.2	All	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	1.0.2	beta1	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	1.0.2	beta2	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	1.0.2	beta3	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	1.0.2a	All	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	1.0.2b	All	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	1.0.2c	All	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	1.0.2d	All	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	1.0.2e	All	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	1.0.2f	All	All	All

## References

Reference	Source	Link
[security-announce] openSUSE-SU-2016:1566-1: important: Security update	SUSE	<a href="#">lists.opensuse.org</a>
Oracle Solaris Bulletin - April 2016	CONFIRM	<a href="#">www.oracle.com</a>
Oracle Critical Patch Update Advisory - April 2016	CONFIRM	<a href="#">www.oracle.com</a>
'[security bulletin] HPSBGN03563 rev.1 - HPE IceWall Products using OpenSSL, Remote Denial of Service' - MARC	HP	<a href="#">marc.info</a>
[security-announce] openSUSE-SU-2016:0637-1: important: Security update	SUSE	<a href="#">lists.opensuse.org</a>
[security-announce] SUSE-SU-2016:0617-1: important: Security update for	SUSE	<a href="#">lists.opensuse.org</a>
Oracle Critical Patch Update - July 2016	CONFIRM	<a href="#">www.oracle.com</a>
[security-announce] openSUSE-SU-2016:0720-1: important: Security update	SUSE	<a href="#">lists.opensuse.org</a>
[security-announce] openSUSE-SU-2016:0627-1: important: Security update	SUSE	<a href="#">lists.opensuse.org</a>
[security-announce] SUSE-SU-2016:0624-1: important: Security update for	SUSE	<a href="#">lists.opensuse.org</a>
[security-announce] SUSE-SU-2016:0620-1: important: Security update for	SUSE	<a href="#">lists.opensuse.org</a>
Oracle July 2016 Critical Patch Update Multiple Vulnerabilities	BID	<a href="#">www.securityadvisories.com</a>
OpenSSL Flaws Let Remote Users Deny Service and Decrypt TLS Sessions in Certain Cases - SecurityTracker	SECTRAK	<a href="#">www.securityadvisories.com</a>

OpenSSL: Multiple vulnerabilities (GLSA 201603-15) — Gentoo Security	GENTOO	<a href="#">security</a>
HPE Support document - HPE Support Center	CONFIRM	<a href="#">h20566</a>
<a href="#">www.openssl.org/news/secadv/20160301.txt</a>	CONFIRM	<a href="#">www.op</a>
[security-announce] SUSE-SU-2016:1057-1: important: Security update for	SUSE	<a href="#">lists.ope</a>
Document Display   HPE Support Center	CONFIRM	<a href="#">h20566</a>
Multiple Vulnerabilities in OpenSSL Affecting Cisco Products: March 2016	CISCO	<a href="#">tools.cis</a>
[security-announce] openSUSE-SU-2016:0638-1: important: Security update	SUSE	<a href="#">lists.ope</a>
[security-announce] SUSE-SU-2016:0678-1: important: Security update for	SUSE	<a href="#">lists.ope</a>
<a href="#">openssl.org/news/secadv/20160301.txt</a>	CONFIRM	<a href="#">openssl</a>
[security-announce] openSUSE-SU-2016:0628-1: important: Security update	SUSE	<a href="#">lists.ope</a>
[security-announce] SUSE-SU-2016:0631-1: important: Security update for	SUSE	<a href="#">lists.ope</a>
[security-announce] openSUSE-SU-2016:1241-1: important: Security update	SUSE	<a href="#">lists.ope</a>
Oracle VM Server for x86 Bulletin - July 2016	CONFIRM	<a href="#">www.or</a>
[security-announce] SUSE-SU-2016:0641-1: important: Security update for	SUSE	<a href="#">lists.ope</a>
OpenSSL CVE-2016-0797 Multiple Integer Overflow Vulnerabilities	BID	<a href="#">www.se</a>
<a href="#">git.openssl.org</a> Git - openssl.git/commit		<a href="#">git.oper</a>
<a href="#">cert-portal.siemens.com/productcert/pdf/ssa-412672.pdf</a>	CONFIRM	<a href="#">cert-por</a>
Oracle Linux Bulletin - January 2016	CONFIRM	<a href="#">www.or</a>
FreeBSD-SA-16:12	FREEBSD	<a href="#">security</a>
<a href="#">git.openssl.org</a> Git - openssl.git/commit	CONFIRM	<a href="#">git.oper</a>
Debian -- Security Information -- DSA-3500-1 openssl	DEBIAN	<a href="#">www.de</a>
[security-announce] SUSE-SU-2016:0621-1: important: Security update for	SUSE	<a href="#">lists.ope</a>
USN-2914-1: OpenSSL vulnerabilities   Ubuntu	UBUNTU	<a href="#">www.ub</a>
Juniper Networks - 2016-10 Security Bulletin: OpenSSL security updates	CONFIRM	<a href="#">kb.junip</a>
Public KB - SA40168 - [Pulse Secure] March 1st 2016 OpenSSL Security Advisory	CONFIRM	<a href="#">kb.pulse</a>
[security-announce] openSUSE-SU-2016:0640-1: important: Security update	SUSE	<a href="#">lists.ope</a>
McAfee Security Bulletin: McAfee Web Gateway update fixes multiple vulnerabilities	CONFIRM	<a href="#">kc.mcaf</a>
Document Display   HPE Support Center	CONFIRM	<a href="#">h20566</a>
[security-announce] openSUSE-SU-2016:1239-1: important: Security update	SUSE	<a href="#">lists.ope</a>
Document Display   HPE Support Center	CONFIRM	<a href="#">h20566</a>
Red Hat Customer Portal	REDHAT	<a href="#">rhn.redh</a>
Oracle Solaris Bulletin - January 2016	CONFIRM	<a href="#">www.or</a>
CVE Program record	CVE.ORG	<a href="#">www.cv</a>
NVD vulnerability detail	NVD	<a href="#">nvd.nist</a>

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)

© [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](#)