



CVE-2015-0289

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

Summary

CVE	CVE-2015-0289
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-03-19 22:59:00 UTC
Updated	2023-11-07 02:23:00 UTC
Description	The PKCS#7 implementation in OpenSSL before 0.9.8zf, 1.0.0 before 1.0.0r, 1.0.1 before 1.0.1m, and 1.0.2 before 1.0.2a c

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Openssl	Openssl	1.0.0	All	All	All
Application	Openssl	Openssl	1.0.0a	All	All	All
Application	Openssl	Openssl	1.0.0b	All	All	All
Application	Openssl	Openssl	1.0.0c	All	All	All
Application	Openssl	Openssl	1.0.0d	All	All	All
Application	Openssl	Openssl	1.0.0e	All	All	All
Application	Openssl	Openssl	1.0.0f	All	All	All
Application	Openssl	Openssl	1.0.0g	All	All	All
Application	Openssl	Openssl	1.0.0h	All	All	All
Application	Openssl	Openssl	1.0.0i	All	All	All
Application	Openssl	Openssl	1.0.0j	All	All	All
Application	Openssl	Openssl	1.0.0k	All	All	All
Application	Openssl	Openssl	1.0.0l	All	All	All
Application	Openssl	Openssl	1.0.0m	All	All	All
Application	Openssl	Openssl	1.0.0n	All	All	All
Application	Openssl	Openssl	1.0.0o	All	All	All
Application	Openssl	Openssl	1.0.0p	All	All	All

Application	Openssl	Openssl	1.0.0q	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	1.0.2	All	All	All
Application	Openssl	Openssl	All	All	All	All
Application	Openssl	Openssl	1.0.0	All	All	All
Application	Openssl	Openssl	1.0.0a	All	All	All
Application	Openssl	Openssl	1.0.0b	All	All	All
Application	Openssl	Openssl	1.0.0c	All	All	All
Application	Openssl	Openssl	1.0.0d	All	All	All
Application	Openssl	Openssl	1.0.0e	All	All	All
Application	Openssl	Openssl	1.0.0f	All	All	All
Application	Openssl	Openssl	1.0.0g	All	All	All
Application	Openssl	Openssl	1.0.0h	All	All	All
Application	Openssl	Openssl	1.0.0i	All	All	All
Application	Openssl	Openssl	1.0.0j	All	All	All
Application	Openssl	Openssl	1.0.0k	All	All	All
Application	Openssl	Openssl	1.0.0l	All	All	All
Application	Openssl	Openssl	1.0.0m	All	All	All
Application	Openssl	Openssl	1.0.0n	All	All	All
Application	Openssl	Openssl	1.0.0o	All	All	All
Application	Openssl	Openssl	1.0.0p	All	All	All
Application	Openssl	Openssl	1.0.0q	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	1.0.2	All	All	All

References

Reference	Source	Link
Red Hat Customer Portal	REDHAT	rht
About the security content of OS X Yosemite v10.10.4 and Security Update 2015-005 - Apple Support	CONFIRM	su
Oracle Bulletin Board Update - January 2015	CONFIRM	w
openSUSE-SU-2015:0554-1: moderate: Security update for openssl	SUSE	lis
FreeBSD-SA-15:06	FREEBSD	w
Red Hat Customer Portal	REDHAT	rht
1202384 – (CVE-2015-0289) CVE-2015-0289 openssl: PKCS7 NULL pointer dereference	CONFIRM	bi
FortiGuard	CONFIRM	w
Red Hat Customer Portal	REDHAT	rht
Oracle Critical Patch Update - October 2015	CONFIRM	w
Gentoo Security	GENTOO	se
Oracle Critical Patch Update - July 2015	CONFIRM	w
'[security bulletin] HPSBMU03409 rev.1 - HP Matrix Operating Environment, Multiple Vulnerabilities' - MARC	HP	m
[security-announce] SUSE-SU-2015:0578-1: important: Security update for	SUSE	lis
OpenSSL 'pk7_doit.c' NULL Pointer Dereference Denial of Service Vulnerability	BID	w
APPLE-SA-2015-06-30-2 OS X Yosemite v10.10.4 and Security Update 2015-005	APPLE	lis
www.openssl.org/news/secadv_20150319.txt	CONFIRM	w
git.openssl.org Git - openssl.git/commit		gi
'[security bulletin] HPSBMU03397 rev.1 - HP Version Control Agent (VCA) on Windows and Linux, Multipl' - MARC	HP	m
Support / Security / Advisories // MDVSA-2015:062 Mandriva	MANDRIVA	w

Support / Security / Advisories // MDVSA-2015:063 Mandriva	MANDRIVA	w
[security-announce] SUSE-SU-2015:0541-1: important: Security update for	SUSE	lis
[SECURITY] Fedora 22 Update: openssl-1.0.1k-6.fc22	FEDORA	lis
[SECURITY] Fedora 20 Update: openssl-1.0.1e-42.fc20	FEDORA	lis
cert-portal.siemens.com/productcert/pdf/ssa-412672.pdf	CONFIRM	co
OpenSSL Multiple Flaws Let Remote Users Deny Service - SecurityTracker	SECTRACK	w
'[security bulletin] HPSBUX03334 SSRT102000 rev.1 - HP-UX Running OpenSSL, Remote Denial of Service (' - MARC	HP	m
[SECURITY] Fedora 21 Update: mingw-openssl-1.0.2a-1.fc21	FEDORA	lis
USN-2537-1: OpenSSL vulnerabilities Ubuntu	UBUNTU	w
2015-04 Security Bulletin: OpenSSL 19th March 2015 advisory - Juniper Networks	CONFIRM	kl
OpenSSL Updates of 19 March 2015 - Red Hat Customer Portal	CONFIRM	ar
[security-announce] openSUSE-SU-2015:1277-1: important: Security update	SUSE	lis
[security-announce] openSUSE-SU-2016:0640-1: important: Security update	SUSE	lis
git.openssl.org Git - openssl.git/commit	CONFIRM	gi
[SECURITY] Fedora 21 Update: openssl-1.0.1k-6.fc21	FEDORA	lis
'[security bulletin] HPSBMU03380 rev.1 - HP System Management Homepage (SMH) on Linux and Windows, Mu' - MARC	HP	m
[SECURITY] Fedora 22 Update: mingw-openssl-1.0.2a-1.fc22	FEDORA	lis
Red Hat Customer Portal	REDHAT	rf
Oracle Solaris Third Party Bulletin - April 2015	CONFIRM	w
Broadcom Support Portal	CONFIRM	bi
Debian -- Security Information -- DSA-3197-1 openssl	DEBIAN	w
Oracle Critical Patch Update - October 2017	CONFIRM	w
'[security bulletin] HPSBGN03306 rev.1 - HP IceWall SSO MCRP, SSO Dfw, and SSO Agent running OpenSSL,' - MARC	HP	m
McAfee KnowledgeBase - Intel Security - Security Bulletin: Fourteen OpenSSL CVEs Announced on March 19, 2015	CONFIRM	kc
Oracle Critical Patch Update - January 2016	CONFIRM	w
CVE Program record	CVE.ORG	w
NVD vulnerability detail	NVD	n

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[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)

[590349](#) Hockwell Automation Stratix 5900 Multiple Vulnerabilities (ICSA-17-094-04)

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

[671109](#) EulerOS Security Update for Open Secure Sockets Layer098e (OpenSSL098e) (EulerOS-SA-2019-2509)

© [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](#)