



CVE-2015-1790

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

Summary

CVE	CVE-2015-1790
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-06-12 19:59:00 UTC
Updated	2022-12-13 12:15:00 UTC
Description	The PKCS7_dataDecodefunction in crypto/pkcs7/pk7_doit.c in OpenSSL before 0.9.8zg, 1.0.0 before 1.0.0s, 1.0.1 before 1

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	1.0.0	beta1	All	All
Application	Openssl	Openssl	1.0.0	beta2	All	All
Application	Openssl	Openssl	1.0.0	beta3	All	All
Application	Openssl	Openssl	1.0.0	beta4	All	All
Application	Openssl	Openssl	1.0.0	beta5	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	1.0.0r	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	1.0.2	All	All	All
Application	Openssl	Openssl	1.0.2	beta1	All	All
Application	Openssl	Openssl	1.0.2a	All	All	All
Application	Openssl	Openssl	All	All	All	All
Application	Openssl	Openssl	1.0.0	All	All	All
Application	Openssl	Openssl	1.0.0	beta1	All	All
Application	Openssl	Openssl	1.0.0	beta2	All	All
Application	Openssl	Openssl	1.0.0	beta3	All	All
Application	Openssl	Openssl	1.0.0	beta4	All	All
Application	Openssl	Openssl	1.0.0	beta5	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	1.0.0r	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	1.0.2	All	All	All

Application	Openssl	Openssl	1.0.2	beta1	All	All
Application	Openssl	Openssl	1.0.2a	All	All	All

References

Reference	Source	Link
Document Display HPE Support Center	CONFIRM	h2056
Oracle Critical Patch Update Advisory - April 2016	CONFIRM	www.o
NetBSD-SA2015-008	NETBSD	ftp.ne
2016-04 Security Bulletin: ScreenOS: Multiple Vulnerabilities in OpenSSL - Juniper Networks	CONFIRM	kb.jun
Oracle Critical Patch Update - July 2016	CONFIRM	www.o
OpenSSL Bugs Let Remote Users Deny Service and Potentially Execute Arbitrary Code - SecurityTracker	SECTRAK	www.s
Oracle July 2016 Critical Patch Update Multiple Vulnerabilities	BID	www.o
USN-2639-1: OpenSSL vulnerabilities Ubuntu	UBUNTU	www.o
Oracle Critical Patch Update - October 2015	CONFIRM	www.o
Document Display HPE Support Center	CONFIRM	h2056
FortiGuard	CONFIRM	www.o
OpenSSL: Multiple vulnerabilities (GLSA 201506-02) — Gentoo security	GENTOO	secur
[SECURITY] Fedora 21 Update: openssl-1.0.1k-10.fc21	FEDORA	lists.fe
About the security content of OS X Yosemite v10.10.5 and Security Update 2015-006 - Apple Support	CONFIRM	suppc
openssl.org/news/secadv/20150611.txt	CONFIRM	opense
Document Display HPE Support Center	CONFIRM	h2056
'[security bulletin] HPSBMU03409 rev.1 - HP Matrix Operating Environment, Multiple Vulnerabilities' - MARC	HP	marc.o
'[security bulletin] HPSBGN03371 rev.1 - HP IceWall Products running OpenSSL, Remote Denial of Servic' - MARC	HP	marc.o
[security-announce] SUSE-SU-2015:1185-1: important: Security update for	SUSE	lists.o
Arista - Security Advisory 0011	MISC	www.o
[security-announce] SUSE-SU-2015:1183-1: important: Security update for	SUSE	lists.o
Oracle Critical Patch Update - October 2016	CONFIRM	www.o
Document Display HPE Support Center	CONFIRM	h2056
Red Hat Customer Portal	REDHAT	rhn.re
Broadcom Support Portal	CONFIRM	bto.bl
Multiple Vulnerabilities in OpenSSL (June 2015) Affecting Cisco Products	CISCO	tools.o
[security-announce] SUSE-SU-2015:1143-1: important: Security update for	SUSE	lists.o
'[security bulletin] HPSBUX03388 SSRT102180 rev.1 - HP-UX running OpenSSL, Remote Disclosure of Infor' - MARC	HP	marc.o
FortiGuard	CONFIRM	www.o
Oracle Solaris Third Party Bulletin - July 2015	CONFIRM	www.o
[SECURITY] Fedora 22 Update: openssl-1.0.1k-10.fc22	FEDORA	lists.fe

PKCS#7: Fix NULL dereference with missing EncryptedContent. · openssl/openssl@59302b6 · GitHub	CONFIRM	github
www.openssl.org/news/secadv_20150611.txt	CONFIRM	www.o
cert-portal.siemens.com/productcert/pdf/ssa-412672.pdf	CONFIRM	cert-p
[security-announce] SUSE-SU-2015:1182-1: important: Security update for	SUSE	lists.o
[security-announce] SUSE-SU-2015:1184-1: important: Security update for	SUSE	lists.o
APPLE-SA-2015-08-13-2 OS X Yosemite v10.10.5 and Security Update 2015-006	APPLE	lists.a
[security-announce] openSUSE-SU-2015:1277-1: important: Security update	SUSE	lists.o
FortiGuard	CONFIRM	fortigu
[security-announce] openSUSE-SU-2016:0640-1: important: Security update	SUSE	lists.o
[security-announce] SUSE-SU-2015:1150-1: important: Security update for	SUSE	lists.o
Debian -- Security Information -- DSA-3287-1 openssl	DEBIAN	www.i
Red Hat Customer Portal	REDHAT	rhn.re
Document Display HPE Support Center	CONFIRM	h2056
McAfee KnowledgeBase - Intel Security - Security Bulletin: Seven OpenSSL CVEs Announced on June 11, 2015	CONFIRM	kc.mc
Document Display HPE Support Center	CONFIRM	h2056
[security-announce] SUSE-SU-2015:1181-1: important: Security update for	SUSE	lists.o
Oracle Critical Patch Update - July 2017	CONFIRM	www.i
Juniper Networks - 2015-10 Security Bulletin: Junos: OpenSSL June-July 2015 advisories - Knowledge Base	CONFIRM	kb.jun
Oracle Critical Patch Update - October 2017	CONFIRM	www.i
OpenSSL CVE-2015-1790 Denial of Service Vulnerability	BID	www.i
[security-announce] openSUSE-SU-2015:1139-1: important: Security update	SUSE	lists.o
Oracle Critical Patch Update - January 2016	CONFIRM	www.i
CVE Program record	CVE.ORG	www.i
NVD vulnerability detail	NVD	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)

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)

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](#)