



CVE-2015-3195

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

Summary

CVE	CVE-2015-3195
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-12-06 20:59:00 UTC
Updated	2023-11-07 02:25:00 UTC
Description	The ASN1_TFLG_COMBINE implementation in crypto/asn1/tasn_dec.c in OpenSSL before 0.9.8zh, 1.0.0 before 1.0.0t, 1.0.0

Risk And Classification

Problem Types: CWE-200

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Apple	Mac Os X	All	All	All	All
Operating System	Apple	Mac Os X	All	All	All	All
Operating System	Canonical	Ubuntu Linux	12.04	All	All	All
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	15.04	All	All	All
Operating System	Canonical	Ubuntu Linux	15.10	All	All	All
Operating System	Canonical	Ubuntu Linux	12.04	All	All	All
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	15.04	All	All	All
Operating System	Canonical	Ubuntu Linux	15.10	All	All	All
Operating System	Debian	Debian Linux	7.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	7.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Fedoraproject	Fedora	22	All	All	All
Operating System	Fedoraproject	Fedora	22	All	All	All
Application	Openssl	Openssl	All	All	All	All

Application	Openssl	Openssl	All	All	All	All
Operating System	Opensuse	Leap	42.1	All	All	All
Operating System	Opensuse	Leap	42.1	All	All	All
Operating System	Opensuse	Opensuse	11.4	All	All	All
Operating System	Opensuse	Opensuse	13.1	All	All	All
Operating System	Opensuse	Opensuse	13.2	All	All	All
Operating System	Opensuse	Opensuse	11.4	All	All	All
Operating System	Opensuse	Opensuse	13.1	All	All	All
Operating System	Opensuse	Opensuse	13.2	All	All	All
Application	Oracle	Api Gateway	11.1.2.3.0	All	All	All
Application	Oracle	Api Gateway	11.1.2.4.0	All	All	All
Application	Oracle	Api Gateway	11.1.2.3.0	All	All	All
Application	Oracle	Api Gateway	11.1.2.4.0	All	All	All
Application	Oracle	Communications Webrtc Session Controller	7.0	All	All	All
Application	Oracle	Communications Webrtc Session Controller	7.1	All	All	All
Application	Oracle	Communications Webrtc Session Controller	7.2	All	All	All
Application	Oracle	Communications Webrtc Session Controller	7.0	All	All	All
Application	Oracle	Communications Webrtc Session Controller	7.1	All	All	All
Application	Oracle	Communications Webrtc Session Controller	7.2	All	All	All
Application	Oracle	Exalogic Infrastructure	1.0	All	All	All
Application	Oracle	Exalogic Infrastructure	2.0	All	All	All
Application	Oracle	Exalogic Infrastructure	1.0	All	All	All
Application	Oracle	Exalogic Infrastructure	2.0	All	All	All
Application	Oracle	Http Server	11.5.10.2	All	All	All
Application	Oracle	Http Server	11.5.10.2	All	All	All
Operating System	Oracle	Integrated Lights Out Manager Firmware	All	All	All	All
Application	Oracle	Life Sciences Data Hub	2.1	All	All	All
Application	Oracle	Life Sciences Data Hub	2.1	All	All	All
Operating System	Oracle	Linux	5	-	All	All
Operating System	Oracle	Linux	6	-	All	All
Operating System	Oracle	Linux	7	-	All	All
Operating System	Oracle	Linux	5	-	All	All
Operating System	Oracle	Linux	6	-	All	All
Operating System	Oracle	Linux	7	-	All	All
Operating System	Oracle	Solaris	10	All	All	All

Operating System	Oracle	Solaris	11.3	All	All	All
Operating System	Oracle	Solaris	10	All	All	All
Operating System	Oracle	Solaris	11.3	All	All	All
Application	Oracle	Sun Ray Software	11.1	All	All	All
Application	Oracle	Sun Ray Software	11.1	All	All	All
Application	Oracle	Transportation Management	6.1	All	All	All
Application	Oracle	Transportation Management	6.2	All	All	All
Application	Oracle	Transportation Management	6.1	All	All	All
Application	Oracle	Transportation Management	6.2	All	All	All
Application	Oracle	Vm Server	3.2	All	All	All
Application	Oracle	Vm Server	3.2	All	All	All
Application	Oracle	Vm Virtualbox	All	All	All	All
Application	Oracle	Vm Virtualbox	All	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	5.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	5.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	5.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	5.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	7.2	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	7.3	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	7.4	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	7.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	7.7	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	7.2	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	7.3	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	7.4	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	7.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	7.7	All	All	All

Operating System	Redhat	Enterprise Linux Server 1 us	7.2	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	7.3	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	7.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	7.7	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	7.2	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	7.3	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	7.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	7.7	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	5.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	5.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	7.0	All	All	All
Operating System	Suse	Linux Enterprise Server	10	sp4	All	All
Operating System	Suse	Linux Enterprise Server	10	sp4	All	All

References

Reference	Source	Li
Oracle Critical Patch Update Advisory - April 2016	CONFIRM	wv
USN-2830-1: OpenSSL vulnerabilities Ubuntu	UBUNTU	wv
APPLE-SA-2016-03-21-5 OS X El Capitan 10.11.4 and Security Update 2016-002	APPLE	list
Multiple Vulnerabilities in OpenSSL (December 2015) Affecting Cisco Products	CISCO	toc
[security-announce] openSUSE-SU-2016:0637-1: important: Security update	SUSE	list
2016-04 Security Bulletin: ScreenOS: Multiple Vulnerabilities in OpenSSL - Juniper Networks	CONFIRM	kb
Oracle Critical Patch Update - July 2016	CONFIRM	wv
openssl.org/news/secadv/20151203.txt	CONFIRM	op
Oracle July 2016 Critical Patch Update Multiple Vulnerabilities	BID	wv
Debian -- Security Information -- DSA-3413-1 openssl	DEBIAN	wv
Red Hat Customer Portal	REDHAT	rhr
FortiGuard.com OpenSSL Advisory - December 2015	CONFIRM	for
Oracle Critical Patch Update - January 2018	CONFIRM	wv
git.openssl.org Git - openssl.git/commit		git
RHSA-2016:2056	REDHAT	rhr
Oracle Critical Patch Update - October 2016	CONFIRM	wv
[security-announce] SUSE-SU-2016:0678-1: important: Security update for	SUSE	list

OpenSSL CVE-2015-3195 Information Disclosure Vulnerability	BID	wv
openSUSE-SU-2015:2288-1: moderate: Security update for OpenSSL	SUSE	list
Document Display HPE Support Center	CONFIRM	h2
[SECURITY] Fedora 22 Update: openssl-1.0.1k-13.fc22	FEDORA	list
Document Display HPE Support Center	CONFIRM	h2
git.openssl.org Git - openssl.git/commit	CONFIRM	git
openSUSE-SU-2015:2289-1: moderate: Security update for openssl	SUSE	list
Oracle VM Server for x86 Bulletin - July 2016	CONFIRM	wv
Document Display HPE Support Center	CONFIRM	h2
Public KB - SA40100 - [Pulse Secure] December 3rd 2015 OpenSSL Security Advisory	CONFIRM	kb
2016-10 Security Bulletin: CTPView: Multiple vulnerabilities in CTPView - Juniper Networks	CONFIRM	kb
'[security bulletin] HPSBGN03536 rev.1 - HP IceWall Products running OpenSSL, Remote and Local Denial' - MARC	HP	ma
Oracle Linux Bulletin - October 2015	CONFIRM	wv
cert-portal.siemens.com/productcert/pdf/ssa-412672.pdf	CONFIRM	ce
Document Display HPE Support Center	CONFIRM	h2
openSUSE-SU-2015:2349-1: moderate: Security update for compat-openssl098	SUSE	list
Document Display HPE Support Center	CONFIRM	h2
FortiGuard.com OpenSSL Advisory - December 2015	CONFIRM	wv
Juniper Networks - 2016-10 Security Bulletin: OpenSSL security updates	CONFIRM	kb
[security-announce] openSUSE-SU-2016:0640-1: important: Security update	SUSE	list
OpenSSL Multiple Bugs Let Remote Users Deny Service and Obtain Potentially Sensitive Information - SecurityTracker	SECTrack	wv
Document Display HPE Support Center	CONFIRM	h2
About the security content of OS X El Capitan v10.11.4 and Security Update 2016-002 - Apple Support	CONFIRM	su
openSUSE-SU-2015:2318-1: moderate: Security update for libressl	SUSE	list
The Slackware Linux Project: Slackware Security Advisories	SLACKWARE	wv
Oracle Critical Patch Update - July 2017	CONFIRM	wv
Oracle Critical Patch Update - October 2017	CONFIRM	wv
Red Hat Customer Portal	REDHAT	rhr
Red Hat Customer Portal	REDHAT	rhr
Oracle Solaris Bulletin - January 2016	CONFIRM	wv
Oracle Critical Patch Update - January 2016	CONFIRM	wv
CVE Program record	CVE.ORG	wv
NVD vulnerability detail	NVD	nv

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[375442](#) HPE System Management Homepage Multiple Vulnerabilities (HPESBMU03593)

[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)

© [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](#)