CVE-2016-0705

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2016-0705
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2016-03-03 20:59:00 UTC
Updated	2023-11-07 02:29:00 UTC
Description	Double free vulnerability in the dsa_priv_decode function in crypto/dsa/dsa_ameth.c in OpenSSL 1.0.1 before 1.0.1s and 1.

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
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	15.10	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	15.10	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	Google	Android	4.0	All	All	All
Operating System	Google	Android	4.0.1	All	All	All
Operating System	Google	Android	4.0.2	All	All	All
Operating System	Google	Android	4.0.3	All	All	All
Operating System	Google	Android	4.0.4	All	All	All
Operating System	Google	Android	4.1	All	All	All
Operating System	Google	Android	4.1.2	All	All	All

Operating System	Google	Android	4.2	All	All	All
Operating System	Google	Android	4.2.1	All	All	All
Operating System	Google	Android	4.2.2	All	All	All
Operating System	Google	Android	4.3	All	All	All
Operating System	Google	Android	4.3.1	All	All	All
Operating System	Google	Android	4.4	All	All	All
Operating System	Google	Android	4.4.1	All	All	All
Operating System	Google	Android	4.4.2	All	All	All
Operating System	Google	Android	4.4.3	All	All	All
Operating System	Google	Android	5.0	All	All	All
Operating System	Google	Android	5.0.1	All	All	All
Operating System	Google	Android	5.1	All	All	All
Operating System	Google	Android	5.1.0	All	All	All
Operating System	Google	Android	6.0	All	All	All
Operating System	Google	Android	6.0.1	All	All	All
Operating System	Google	Android	4.0	All	All	All
Operating System	Google	Android	4.0.1	All	All	All
Operating System	Google	Android	4.0.2	All	All	All
Operating System	Google	Android	4.0.3	All	All	All
Operating System	Google	Android	4.0.4	All	All	All
Operating System	Google	Android	4.1	All	All	All
Operating System	Google	Android	4.1.2	All	All	All
Operating System	Google	Android	4.2	All	All	All
Operating System	Google	Android	4.2.1	All	All	All
Operating System	Google	Android	4.2.2	All	All	All
Operating System	Google	Android	4.3	All	All	All
Operating System	Google	Android	4.3.1	All	All	All
Operating System	Google	Android	4.4	All	All	All
Operating System	Google	Android	4.4.1	All	All	All
Operating System	Google	Android	4.4.2	All	All	All
Operating System	Google	Android	4.4.3	All	All	All
Operating System	Google	Android	5.0	All	All	All
Operating System	Google	Android	5.0.1	All	All	All
Operating System	Google	Android	5.1	All	All	All
Operating System	Google	Android	5.1.0	All	All	All

Operating System	Google	Android	6.0	All	All	All
Operating System	Google	Android	6.0.1	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
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	Oracle	Mysql	All	All	All	All
Application	Oracle	Mysql	All	All	All	All

References

Reference	Source	Link

[security-announce] openSUSE-SU-2016:1566-1: important: Security update	SUSE	lists.o
Oracle Solaris Bulletin - April 2016	CONFIRM	www.
Oracle Critical Patch Update Advisory - April 2016	CONFIRM	www.
'[security bulletin] HPSBGN03563 rev.1 - HPE IceWall Products using OpenSSL, Remote Denial of Service' - MARC	HP	marc.
[security-announce] openSUSE-SU-2016:0637-1: important: Security update	SUSE	lists.o
[security-announce] SUSE-SU-2016:0617-1: important: Security update for	SUSE	lists.o
Oracle Critical Patch Update - July 2016	CONFIRM	www.
OpenSSL CVE-2016-0705 Denial of Service Vulnerability	BID	www.
HPE Support document - HPE Support Center	CONFIRM	h2056
[security-announce] openSUSE-SU-2016:0627-1: important: Security update	SUSE	lists.o
[security-announce] SUSE-SU-2016:0624-1: important: Security update for	SUSE	lists.o
[security-announce] SUSE-SU-2016:0620-1: important: Security update for	SUSE	lists.o
Oracle July 2016 Critical Patch Update Multiple Vulnerabilities	BID	www.
OpenSSL Flaws Let Remote Users Deny Service and Decrypt TLS Sessions in Certain Cases - SecurityTracker	SECTRACK	www.
Document Display | HPE Support Center	CONFIRM	h2056
OpenSSL: Multiple vulnerabilities (GLSA 201603-15) — Gentoo Security	GENTOO	secur
HPE Support document - HPE Support Center	CONFIRM	h2056
www.openssl.org/news/secadv/20160301.txt	CONFIRM	www.
Document Display | HPE Support Center	CONFIRM	h2056
[security-announce] SUSE-SU-2016:1057-1: important: Security update for	SUSE	lists.o
Document Display | HPE Support Center	CONFIRM	h2056
Red Hat Customer Portal	REDHAT	acces
Multiple Vulnerabilities in OpenSSL Affecting Cisco Products: March 2016	CISCO	tools.
git.openssl.org Git - openssl.git/commit		git.op
[security-announce] openSUSE-SU-2016:0638-1: important: Security update	SUSE	lists.o
'[security bulletin] HPSBMU03575 rev.1 - HP Smart Update Manager (SUM), Remote Denial of Service (DoS' - MARC	HP	marc.
openssl.org/news/secadv/20160301.txt	CONFIRM	opens
Document Display | HPE Support Center	CONFIRM	h2056
git.openssl.org Git - openssl.git/commit	CONFIRM	git.op
[security-announce] openSUSE-SU-2016:0628-1: important: Security update	SUSE	lists.o
[security-announce] SUSE-SU-2016:0631-1: important: Security update for	SUSE	lists.o
Document Display | HPE Support Center	CONFIRM	h2056
Android Security Bulletin—May 2016 | Android Open Source Project	CONFIRM	sourc
Document Display | HPE Support Center	CONFIRM	h2056
HPE Support document - HPE Support Center	CONFIRM	h2056
Red Hat Customer Portal	REDHAT	acces

Red Hat Customer Portal	REDHAT	acces
cert-portal.siemens.com/productcert/pdf/ssa-412672.pdf	CONFIRM	cert-p
Document Display | HPE Support Center	CONFIRM	h2056
Oracle Linux Bulletin - January 2016	CONFIRM	www.
FreeBSD-SA-16:12	FREEBSD	secur
Document Display | HPE Support Center	CONFIRM	h2056
Debian -- Security Information -- DSA-3500-1 openssl	DEBIAN	www.
[security-announce] SUSE-SU-2016:0621-1: important: Security update for	SUSE	lists.o
USN-2914-1: OpenSSL vulnerabilities | Ubuntu	UBUNTU	www.
Juniper Networks - 2016-10 Security Bulletin: OpenSSL security updates	CONFIRM	kb.jur
Public KB - SA40168 - [Pulse Secure] March 1st 2016 OpenSSL Security Advisory	CONFIRM	kb.pu
Document Display | HPE Support Center	CONFIRM	h2056
Document Display | HPE Support Center	CONFIRM	h2056
Document Display | HPE Support Center	CONFIRM	h2056
Document Display | HPE Support Center	CONFIRM	h2056
Red Hat Customer Portal	REDHAT	acces
Document Display | HPE Support Center	CONFIRM	h2056
[SECURITY] Fedora 22 Update: openssl-1.0.1k-14.fc22	FEDORA	lists.fe
[security-announce] openSUSE-SU-2016:1332-1: important: Security update	SUSE	lists.o
Document Display | HPE Support Center	CONFIRM	h2056
Red Hat Customer Portal	REDHAT	rhn.re
'[security bulletin] HPSBGN03569 rev.1 - HPE OneView for VMware vCenter (OV4VC), Remote Disclosure of' - MARC	HP	marc.
[SECURITY] Fedora 23 Update: openssl-1.0.2g-2.fc23	FEDORA	lists.fe
CVE Program record	CVE.ORG	www.
NVD vulnerability detail	NVD	nvd.n

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

375442 HPE System Management Homepage Multiple Vulnerabilities (HPESBMU03593)

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)