CVE-2016-2108

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2016-2108
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2016-05-05 01:59:00 UTC
Updated	2023-11-07 02:30:00 UTC
Description	The ASN.1 implementation in OpenSSL before 1.0.1o and 1.0.2 before 1.0.2c allows remote attackers to execute arbitrary

Risk And Classification

Problem Types: CWE-119

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
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	1.0.2	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	1.0.2	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	All	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	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Hpc Node	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Hpc Node	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Hpc Node	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Hpc Node	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Hpc Node Eus	7.2	All	All	All
Operating System	Redhat	Enterprise Linux Hpc Node Eus	7.2	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	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	7.2	All	All	All
Operating System	Redhat	Enterprise Linux Server Eus	7.2	All	All	All
Operating System	Redhat	Enterprise Linux Server Eus	7.2	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	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	7.0	All	All	All

References

Reference
Oracle Solaris Bulletin - April 2016
USN-2959-1: OpenSSL vulnerabilities | Ubuntu
[security-announce] SUSE-SU-2016:1231-1: important: Security update for
[security-announce] openSUSE-SU-2016:1238-1: important: Security update
About the security content of OS X El Capitan v10.11.6 and Security Update 2016-004 - Apple Support
[security-announce] openSUSE-SU-2016:1237-1: important: Security update

Document Display | HPE Support Center
[security-announce] openSUSE-SU-2016:1273-1: important: Security update
Slackware Security Advisory - openssl Updates ≈ Packet Storm
git.openssl.org Git - openssl.git/commit
Oracle Critical Patch Update - July 2016
git.openssl.org Git - openssl.git/commit
[security-announce] SUSE-SU-2016:1360-1: important: Security update for
git.openssl.org Git - openssl.git/commit
APPLE-SA-2016-07-18-1 OS X El Capitan v10.11.6 and Security Update 2016-004
Red Hat Customer Portal
Red Hat Customer Portal
Oracle July 2016 Critical Patch Update Multiple Vulnerabilities
[security-announce] SUSE-SU-2016:1233-1: important: Security update for
[security-announce] SUSE-SU-2016:1206-1: important: Security update for
Broadcom Support Portal
[security-announce] openSUSE-SU-2016:1242-1: important: Security update
RHSA-2016:2056
[security-announce] SUSE-SU-2016:1290-1: important: Security update for
[security-announce] openSUSE-SU-2016:1240-1: important: Security update
OpenSSL CVE-2016-2108 ASN.1 Encoder Remote Memory Corruption Vulnerability
[R7] LCE 4.8.1 Fixes Multiple Vulnerabilities - Security Advisory | Tenable™
[SECURITY] Fedora 22 Update: openssl-1.0.1k-15.fc22
Document Display | HPE Support Center
Oracle Linux Bulletin - April 2016
[security-announce] openSUSE-SU-2016:1241-1: important: Security update
Document Display | HPE Support Center
[SECURITY] Fedora 23 Update: openssl-1.0.2h-1.fc23
Document Display | HPE Support Center
OpenSSL: Multiple vulnerabilities (GLSA 201612-16) — Gentoo security
The Slackware Linux Project: Slackware Security Advisories
OpenSSL Multiple Bugs Let Remote Users Decrypt Data, Deny Service, Obtain Potentially Sensitive Information, and Potentially Execute Arbi
git.openssl.org Git - openssl.git/commit
Android Security Bulletin—July 2016 | Android Open Source Project
[security-announce] SUSE-SU-2016:1267-1: important: Security update for
Security Center

Red Hat Customer Portal
[security-announce] openSUSE-SU-2016:1243-1: important: Security update
Red Hat Customer Portal
cert-portal.siemens.com/productcert/pdf/ssa-412672.pdf
Red Hat Customer Portal
[security-announce] SUSE-SU-2016:1228-1: important: Security update for
Document Display | HPE Support Center
Multiple Vulnerabilities in OpenSSL Affecting Cisco Products: May 2016
Red Hat Customer Portal
www.openssl.org/news/secadv/20160503.txt
[SECURITY] Fedora 24 Update: openssl-1.0.2h-1.fc24
Juniper Networks - 2016-10 Security Bulletin: OpenSSL security updates
May 2016 OpenSSL Vulnerabilities in Multiple NetApp Products | NetApp Product Security
Public KB - SA40202 - [Pulse Secure] May 3rd 2016 OpenSSL Security Advisory
Document Display | HPE Support Center
[security-announce] openSUSE-SU-2016:1239-1: important: Security update
Oracle Critical Patch Update - July 2017
Citrix XenServer Multiple Security Updates
Red Hat Customer Portal
Debian -- Security Information -- DSA-3566-1 openssl
CVE Program record
NVD vulnerability detail

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)

43588 Huawei Open Secure Sockets Layer (OpenSSL) Multiple Vulnerabilities (huawei-sa-20160706-01-openssl)

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

CVE.report and Source URL Uptime Status status.cve.report