CVE-2015-0286

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2015-0286
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 ASN1_TYPE_cmp function in crypto/asn1/a_type.c in OpenSSL before 0.9.8zf, 1.0.0 before 1.0.0r, 1.0.1 before 1.0.1m

Risk And Classification

Problem Types: CWE-17

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
Red Hat Customer Portal
APPLE-SA-2015-09-16-1 iOS 9
About the security content of OS X Yosemite v10.10.4 and Security Update 2015-005 - Apple Support
Oracle Bulletin Board Update - January 2015
1202366 – (CVE-2015-0286) CVE-2015-0286 openssl: invalid pointer use in ASN1_TYPE_cmp()
openSUSE-SU-2015:0554-1: moderate: Security update for openssl
FreeBSD-SA-15:06
Red Hat Customer Portal
APPLE-SA-2015-09-30-3 OS X El Capitan 10.11
FortiGuard
Oracle Critical Patch Update - October 2015
Multiple Security Vulnerabilities in Citrix NetScaler Platform IPMI Lights Out Management (LOM) firmware
Oracle Critical Patch Update - July 2015
'[security bulletin] HPSBMU03409 rev.1 - HP Matrix Operating Environment, Multiple Vulnerabilities' - MARC
[security-announce] SUSE-SU-2015:0578-1: important: Security update for
OpenSSL 'ASN1_TYPE_cmp()' Function Denial of Service Vulnerability
Oracle Critical Patch Update - October 2016
APPLE-SA-2015-06-30-2 OS X Yosemite v10.10.4 and Security Update 2015-005
www.openssl.org/news/secadv_20150319.txt
Oracle PeopleSoft Products Lets Local Users Gain Elevated Privileges and Remote Users Partially Access Data and Partially Deny Service - S

'[security bulletin] HPSBMU03397 rev.1 - HP Version Control Agent (VCA) on Windows and Linux, Multipl' - MARC
About the security content of iOS 9 - Apple Support
git.openssl.org Git - openssl.git/commit
Support / Security / Advisories / / MDVSA-2015:062 | Mandriva
Support / Security / Advisories / / MDVSA-2015:063 | Mandriva
git.openssl.org Git - openssl.git/commit
[security-announce] SUSE-SU-2015:0541-1: important: Security update for
[SECURITY] Fedora 22 Update: openssl-1.0.1k-6.fc22
[SECURITY] Fedora 20 Update: openssl-1.0.1e-42.fc20
cert-portal.siemens.com/productcert/pdf/ssa-412672.pdf
OpenSSL Multiple Flaws Let Remote Users Deny Service - SecurityTracker
'[security bulletin] HPSBUX03334 SSRT102000 rev.1 - HP-UX Running OpenSSL, Remote Denial of Service (' - MARC
[SECURITY] Fedora 21 Update: mingw-openssl-1.0.2a-1.fc21
USN-2537-1: OpenSSL vulnerabilities | Ubuntu
2015-04 Security Bulletin: OpenSSL 19th March 2015 advisory - Juniper Networks
OpenSSL Updates of 19 March 2015 - Red Hat Customer Portal
[security-announce] openSUSE-SU-2015:1277-1: important: Security update
[security-announce] openSUSE-SU-2016:0640-1: important: Security update
[SECURITY] Fedora 21 Update: openssl-1.0.1k-6.fc21
'[security bulletin] HPSBMU03380 rev.1 - HP System Management Homepage (SMH) on Linux and Windows, Mu' - MARC
[SECURITY] Fedora 22 Update: mingw-openssl-1.0.2a-1.fc22
'[security bulletin] HPSBMU03413 rev.1 - HP Virtual Connect Enterprise Manager SDK, Multiple Vulnerab' - MARC
About the security content of OS X El Capitan v10.11 - Apple Support
Red Hat Customer Portal
Oracle Solaris Third Party Bulletin - April 2015
Broadcom Support Portal
Debian -- Security Information -- DSA-3197-1 openssl
Oracle Critical Patch Update - July 2017
Oracle Critical Patch Update - October 2017
'[security bulletin] HPSBGN03306 rev.1 - HP IceWall SSO MCRP, SSO Dfw, and SSO Agent running OpenSSL,' - MARC
Red Hat Customer Portal
McAfee KnowledgeBase - Intel Security - Security Bulletin: Fourteen OpenSSL CVEs Announced on March 19, 2015
Oracle Critical Patch Update - January 2016
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)

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