CVE-2015-1789

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2015-1789
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-06-12 19:59:00 UTC
Updated	2023-02-13 00:46:00 UTC
Description	The X509_cmp_time function in crypto/x509/x509_vfy.c in OpenSSL before 0.9.8zg, 1.0.0 before 1.0.0s, 1.0.1 before 1.0.1r

Risk And Classification

Problem Types: CWE-119

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
Application	Oracle	Sparc-opl Service Processor	All	All	All	All

References

Reference	Source	Link
Document Display | HPE Support Center	CONFIRM	h2056
Oracle Critical Patch Update Advisory - April 2016	CONFIRM	www.
NetBSD-SA2015-008	NETBSD	ftp.ne
1228603 – (CVE-2015-1789) CVE-2015-1789 OpenSSL: out-of-bounds read in X509_cmp_time	MISC	bugzil
2016-04 Security Bulletin: ScreenOS: Multiple Vulnerabilities in OpenSSL - Juniper Networks	CONFIRM	kb.jun
Oracle Critical Patch Update - July 2016	CONFIRM	www.
OpenSSL CVE-2015-1789 Out of Bounds Read Denial of Service Vulnerability	BID	www.
HPE Support document - HPE Support Center	CONFIRM	h2056
OpenSSL Bugs Let Remote Users Deny Service and Potentially Execute Arbitrary Code - SecurityTracker	SECTRACK	www.
Oracle July 2016 Critical Patch Update Multiple Vulnerabilities	BID	www.
USN-2639-1: OpenSSL vulnerabilities | Ubuntu	UBUNTU	www.
Oracle Critical Patch Update - October 2015	CONFIRM	www.
Document Display | HPE Support Center	CONFIRM	h2056
FortiGuard	CONFIRM	www.
OpenSSL: Multiple vulnerabilities (GLSA 201506-02) — Gentoo security	GENTOO	securi
Multiple Security Vulnerabilities in Citrix NetScaler Platform IPMI Lights Out Management (LOM) firmware	CONFIRM	suppo
[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	suppo
openssl.org/news/secadv/20150611.txt	CONFIRM	opens
Document Display | HPE Support Center	CONFIRM	h2056
'[security bulletin] HPSBMU03409 rev.1 - HP Matrix Operating Environment, Multiple Vulnerabilities' - MARC	HP	marc.
'[security bulletin] HPSBGN03371 rev.1 - HP IceWall Products running OpenSSL, Remote Denial of Servic' - MARC	HP	marc.
[security-announce] SUSE-SU-2015:1185-1: important: Security update for	SUSE	lists.o
Arista - Security Advisory 0011	MISC	www.
[security-announce] SUSE-SU-2015:1183-1: important: Security update for	SUSE	lists.o
Oracle Critical Patch Update - October 2016	CONFIRM	www.
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.

[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.
access.redhat.com | CVE-2015-1789	MISC	acces
FortiGuard	CONFIRM	www.
Oracle Solaris Third Party Bulletin - July 2015	CONFIRM	www.
Red Hat Customer Portal	MISC	acces
[SECURITY] Fedora 22 Update: openssl-1.0.1k-10.fc22	FEDORA	lists.fe
www.openssl.org/news/secadv_20150611.txt	CONFIRM	www.
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
Red Hat Customer Portal	MISC	acces
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
Fix length checks in X509_cmp_time to avoid out-of-bounds reads. · openssl/openssl@f48b83b · GitHub	CONFIRM	github
[security-announce] SUSE-SU-2015:1150-1: important: Security update for	SUSE	lists.o
Debian -- Security Information -- DSA-3287-1 openssl	DEBIAN	www.
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.
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.
[security-announce] openSUSE-SU-2015:1139-1: important: Security update	SUSE	lists.o
Oracle Critical Patch Update - January 2016	CONFIRM	www.
CVE Program record	CVE.ORG	www.
NVD vulnerability detail	NVD	nvd.ni

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)

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