CVE-2013-6449

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2013-6449
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2013-12-23 22:55:00 UTC
Updated	2023-11-07 02:17:00 UTC
Description	The ssl_get_algorithm2 function in ssl/s3_lib.c in OpenSSL before 1.0.2 obtains a certain version number from an incorrect

Risk And Classification

Problem Types: CWE-310

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	1.0.1	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	1.0.0	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	1.0.1	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	All	All	All	All

References

Reference

USN-2079-1: OpenSSL vulnerabilities | Ubuntu
[TS-2355] ATS 4.0.x crashes when using OpenSSL 1.0.1e - ASF JIRA
Debian -- Security Information -- DSA-2833-1 openssl
[SECURITY] Fedora 19 Update: openssl-1.0.1e-39.fc19
VMSA-2014-0012 | United States
openSUSE-SU-2014:0015-1: moderate: update for openssl
Red Hat Customer Portal
OpenSSL 'ssl_get_algorithm2()' Function Remote Denial of Service Vulnerability
OpenSSL Incorrect Version Number Used in ssl_get_algorithm2() Lets Remote Users Deny Service - SecurityTracker
IBM Tivoli Composite Application Manager for Transactions Internet Service Monitoring 7.3.0.1 Interim Fix 29 README Tivoli Composite Appl
openSUSE-SU-2014:0012-1: moderate: update for openssl
[SECURITY] Fedora 18 Update: openssl-1.0.1e-36.fc18
#3200: Crash in OpenSSL 1.0.1e w/TLS 1.2 (under load)
Oracle Critical Patch Update - January 2015
Full Disclosure: NEW: VMSA-2014-0012 - VMware vSphere product updates address security vulnerabilities
OpenSSL: Multiple vulnerabilities (GLSA 201412-39) — Gentoo Security
git.openssl.org Git - openssl.git/commit
[SECURITY] Fedora 20 Update: openssl-1.0.1e-36.fc20
[SECURITY] Fedora 19 Update: openssl-1.0.1e-36.fc19
IBM Tivoli Composite Application Manager for Transactions Internet Service Monitoring 7.4 Interim Fix 13 README Tivoli Composite Applicati
git.openssl.org Git - openssl.git/commit
Bug 1045363 – CVE-2013-6449 openssl: crash when using TLS 1.2 caused by use of incorrect hash algorithm
Oracle Critical Patch Update - July 2014
openSUSE-SU-2014:0018-1: moderate: update for openssl
openSUSE-SU-2014:0048-1: moderate: update for openssl
SecurityFocus
[SECURITY] Fedora 20 Update: openssl-1.0.1e-39.fc20
Red Hat Customer Portal
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)

591311 Bosch Rexroth PRA-ES8P2S Ethernet-Switch Multiple Vulnerabilities (BOSCH-SA-247053-BT)