CVE-2014-3509

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2014-3509
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-08-13 23:55:00 UTC
Updated	2023-11-07 02:20:00 UTC
Description	Race condition in the ssl_parse_serverhello_tlsext function in t1_lib.c in OpenSSL 1.0.0 before 1.0.0n and 1.0.1 before 1.0.

Risk And Classification

Problem Types: CWE-362

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	1.0.1	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	1.0.0	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	1.0.1	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

References

Reference
About Secunia Research | Flexera
'[security bulletin] HPSBHF03293 rev.1 - HP Virtual Connect 8Gb 24-Port FC Module running OpenSSL and' - MARC
'[security bulletin] HPSBMU03267 rev.1 - HP Matrix Operating Environment and HP CloudSystem Matrix ru' - MARC
'[security bulletin] HPSBMU03263 rev.3 - HP Insight Control running OpenSSL, Remote Disclosure of Inf' - MARC
www.openssl.org/news/secadv_20140806.txt
About Secunia Research | Flexera
About Secunia Research | Flexera
'[security bulletin] HPSBMU03216 rev.2 - HP Service Manager running SSLv3, Multiple Remote Vulnerabil' - MARC
Security Bulletin: Multiple Vulnerabilities in Current Release of IBM® SDK for Node.js™
Security Advisory-9 OpenSSL Vulnerabilities on Huawei products - Huawei PSIRT
[SECURITY] Fedora 19 Update: openssl-1.0.1e-39.fc19
IBM X-Force Exchange
Multiple Security Vulnerabilities in Citrix NetScaler Platform IPMI Lights Out Management (LOM) firmware
Security Advisory SA61184 - IBM SDK for Node.js Multiple Vulnerabilities - Secunia
Red Hat Customer Portal
IBM Security Bulletin: - United States
Security Advisory SA61100 - syslog-ng Premium Edition OpenSSL Multiple Vulnerabilities - Secunia
Security Advisory SA60221 - SUSE update for openssl - Secunia
Document Display | HPE Support Center
OpenSSL Bugs Let Remote Users Deny Service, Obtain Information, and Potentially Execute Arbitrary Code - SecurityTracker
git.openssl.org Git - openssl.git/commit
www.mandriva.com
NetBSD-SA2014-008

OpenSSL: Multiple vulnerabilities (GLSA 201412-39) — Gentoo Security
Security Advisory SA61775 - Huawei Multiple Products Multiple OpenSSL Vulnerabilities - Secunia
Debian -- Security Information -- DSA-2998-1 openssl
About Secunia Research | Flexera
OpenSSL Vulnerabilities related to Version 1.0.1i | Techzone
linux.oracle.com | ELSA-2014-1052
git.openssl.org Git - openssl.git/commit
About Secunia Research | Flexera
IBM notice: The page you requested cannot be displayed
About Secunia Research | Flexera
FreeBSD-SA-14:18
[syslog-ng-announce] syslog-ng Premium Edition 5 LTS (5.0.6a) has been released
Security Advisory SA61959 - IBM Tivoli Management Framework Multiple Vulnerabilities - Secunia
About Secunia Research | Flexera
Security Advisory SA60493 - IBM i OpenSSL Multiple Vulnerabilities - Secunia
About Secunia Research | Flexera
About Secunia Research | Flexera
IBM Security Bulletin: Multiple vulnerabilities in OpenSSL affect IBM Tivoli Composite Application Manager for Transactions (CVE-2014-3508,
Security Advisory SA60938 - NetBSD update for openssl - Secunia
About Secunia Research | Flexera
'[security bulletin] HPSBMU03304 rev.1 - HP Insight Control server deployment on Linux and Windows, R' - MARC
Security Advisory SA60803 - SUSE update for openssl1 - Secunia
aix.software.ibm.com/aix/efixes/security/openssl_advisory10.asc
OpenSSL CVE-2014-3509 Remote Denial of Service Vulnerability
openSUSE-SU-2014:1052-1: moderate: update for openssl
Document Display | HPE Support Center
[SECURITY] Fedora 20 Update: openssl-1.0.1e-39.fc20
'[security bulletin] HPSBMU03260 rev.1 - HP System Management Homepage running OpenSSL on Linux and W' - MARC
1127498 – (CVE-2014-3509) CVE-2014-3509 openssl: race condition in ssl_parse_serverhello_tlsext
'[security bulletin] HPSBMU03261 rev.2 - HP Systems Insight Manager running OpenSSL on Linux and Wind' - MARC
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)