CVE-2015-7575

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2015-7575
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2016-01-09 02:59:00 UTC
Updated	2018-10-30 16:27:00 UTC
Description	Mozilla Network Security Services (NSS) before 3.20.2, as used in Mozilla Firefox before 43.0.2 and Firefox ESR 38.x befo

Risk And Classification

Problem Types: CWE-19

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	15.04	All	All	All
Operating System	Canonical	Ubuntu Linux	15.10	All	All	All
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	15.04	All	All	All
Operating System	Canonical	Ubuntu Linux	15.10	All	All	All
Application	Mozilla	Firefox	All	All	All	All
Application	Mozilla	Firefox Esr	38.0	All	All	All
Application	Mozilla	Firefox Esr	38.0.1	All	All	All
Application	Mozilla	Firefox Esr	38.0.5	All	All	All
Application	Mozilla	Firefox Esr	38.1.0	All	All	All
Application	Mozilla	Firefox Esr	38.1.1	All	All	All
Application	Mozilla	Firefox Esr	38.2.0	All	All	All
Application	Mozilla	Firefox Esr	38.2.1	All	All	All
Application	Mozilla	Firefox Esr	38.3.0	All	All	All
Application	Mozilla	Firefox Esr	38.4.0	All	All	All
Application	Mozilla	Firefox Esr	38.5.0	All	All	All

Application	Mozilla	Firefox Esr	38.5.1	All	All	All
Application	Mozilla	Firefox Esr	38.0	All	All	All
Application	Mozilla	Firefox Esr	38.0.1	All	All	All
Application	Mozilla	Firefox Esr	38.0.5	All	All	All
Application	Mozilla	Firefox Esr	38.1.0	All	All	All
Application	Mozilla	Firefox Esr	38.1.1	All	All	All
Application	Mozilla	Firefox Esr	38.2.0	All	All	All
Application	Mozilla	Firefox Esr	38.2.1	All	All	All
Application	Mozilla	Firefox Esr	38.3.0	All	All	All
Application	Mozilla	Firefox Esr	38.4.0	All	All	All
Application	Mozilla	Firefox Esr	38.5.0	All	All	All
Application	Mozilla	Firefox Esr	38.5.1	All	All	All
Application	Mozilla	Network Security Services	All	All	All	All
Operating System	Opensuse	Leap	42.1	All	All	All
Operating System	Opensuse	Leap	42.1	All	All	All
Operating System	Opensuse	Opensuse	13.1	All	All	All
Operating System	Opensuse	Opensuse	13.2	All	All	All
Operating System	Opensuse	Opensuse	13.1	All	All	All
Operating System	Opensuse	Opensuse	13.2	All	All	All

References

Reference
[security-announce] openSUSE-SU-2016:0263-1: critical: Security update f
Oracle Critical Patch Update Advisory - April 2016
USN-2865-1: GnuTLS vulnerability | Ubuntu
Mozilla Firefox MD5 Signature Support in TLS ServerKeyExchange Messages Exposes Users to Hash Collision Forgery Attacks - SecurityTra
openSUSE-SU-2016:0162-1: moderate: Security update for mbedtls
Oracle Critical Patch Update - July 2016
openSUSE-SU-2016:0488-1: moderate: Security update for Thunderbird
Oracle July 2016 Critical Patch Update Multiple Vulnerabilities
USN-2904-1: Thunderbird vulnerabilities | Ubuntu
NSS 3.20.2 release notes - Mozilla | MDN
[security-announce] SUSE-SU-2016:0265-1: critical: Security update for j
Debian -- Security Information -- DSA-3436-1 openssl
USN-2864-1: NSS vulnerability | Ubuntu

[security-announce] openSUSE-SU-2016:0270-1: critical: Security update f

Red Hat Customer Portal

openSUSE-SU-2015:2405-1: moderate: Security update for mozilla-nss

openSUSE-SU-2016:0308-1: moderate: Security update for Seamonkey

Red Hat Customer Portal

MD5 signatures accepted within TLS 1.2 ServerKeyExchange in server signature — Mozilla

Debian -- Security Information -- DSA-3688-1 nss

Mozilla Network Security Services CVE-2015-7575 Security Bypass Vulnerability

[security-announce] SUSE-SU-2016:0256-1: critical: Security update for j

mbed TLS: Multiple vulnerabilities (GLSA 201706-18) — Gentoo Security

IBM AIX Default TLS Version Lets Remote Users Conduct Man-in-the-Middle Attacks Obtain Potentially Sensitive Information on the Target S

Red Hat Customer Portal

openSUSE-SU-2016:0605-1: moderate: Security update for bouncycastle

Debian -- Security Information -- DSA-3465-1 openjdk-6

openSUSE-SU-2016:0161-1: moderate: Security update for polarssl

USN-2884-1: OpenJDK 7 vulnerabilities | Ubuntu

[security-announce] openSUSE-SU-2016:0272-1: important: Security update

Mozilla Network Security Service (NSS): Multiple vulnerabilities (GLSA 201701-46) — Gentoo security

openSUSE-SU-2016:0007-1: moderate: Security update for MozillaFirefox

Oracle Linux Bulletin - January 2016

Debian -- Security Information -- DSA-3457-1 iceweasel

Red Hat Customer Portal

Red Hat Customer Portal

openSUSE-SU-2016:0307-1: moderate: Security update for seamonkey

Debian -- Security Information -- DSA-3458-1 openjdk-7

[security-announce] openSUSE-SU-2016:0268-1: critical: Security update f

Red Hat Customer Portal

Red Hat Customer Portal

CVE-2015-7575 TLS Vulnerability in Multiple NetApp Products | NetApp Product Security

Debian -- Security Information -- DSA-3437-1 gnutls26

[security-announce] openSUSE-SU-2016:0279-1: critical: Security update f

Access Denied

PolarSSL: Multiple vulnerabilities (GLSA 201801-15) — Gentoo security

USN-2863-1: OpenSSL vulnerability | Ubuntu

[security-announce] SUSE-SU-2016:0269-1: critical: Security update for j

Oracle Critical Patch Update - October 2017

USN-2866-1: Firefox vulnerability | Ubuntu
Oracle Critical Patch Update - January 2016
Debian -- Security Information -- DSA-3491-1 icedove
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)

710439 Gentoo Linux mbed Transport Layer Security (TLS) Multiple Vulnerabilities (GLSA 201706-18)

710518 Gentoo Linux Mozilla Network Security Service (NSS) Multiple Vulnerabilities (GLSA 201701-46)