CVE-2014-1490

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2014-1490
State	PUBLISHED
Assigner	mozilla
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-02-06 05:44:25 UTC
Updated	2026-04-29 01:13:23 UTC
Description	Race condition in libssl in Mozilla Network Security Services (NSS) before 3.15.4, as used in Mozilla Firefox before 27.0, Fi

Risk And Classification

Primary CVSS: v2.0 9.3 from nvd@nist.gov

AV:N/AC:M/Au:N/C:C/I:C/A:C

Problem Types: CWE-362 | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Medium

Authentication

None

Confidentiality

Complete

Integrity

Complete

Availability

Complete

AV:N/AC:M/Au:N/C:C/I:C/A:C

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Mozilla	Firefox	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Na	N/a	affected n/a	Not specified

References

Reference
2016-10 Security Bulletin: CTPView: Multiple vulnerabilities in CTPView - Juniper Networks
MFSA 2014-12: NSS ticket handling issues
Mozilla Thunderbird Multiple Bugs Let Remote Users Execute Arbitrary Code and Obtain Potentially Sensitive Information - SecurityTracker
[security-announce] SUSE-SU-2014:0248-1: important: Security update for
Gentoo Security
Security Advisory SA56922 - SUSE update for Multiple Mozilla Packages - Secunia
Security Advisory SA56706 - Cyberfox Multiple Vulnerabilities - Secunia
Mozilla Firefox Multiple Flaws Let Remote Users Execute Arbitrary Code and Obtain Potentially Sensitive Information - SecurityTracker
[SECURITY] Fedora 20 Update: thunderbird-24.3.0-1.fc20
Oracle VM Server for x86 Bulletin - July 2016
[SECURITY] Fedora 19 Update: thunderbird-24.3.0-1.fc19
Oracle Critical Patch Update - October 2014
Security Advisory SA56888 - Ubuntu update for firefox - Secunia
930874 – (CVE-2014-1490) TOCTOU, potential use-after-free in libssl's session ticket processing due to lack of lock protecting the sessionTic
Mozilla Seamonkey Multiple Bugs Let Remote Users Execute Arbitrary Code and Obtain Potentially Sensitive Information - SecurityTracker
Mozilla Network Security Services CVE-2014-1490 Use After Free Memory Corruption Vulnerability
930857 – NewSessionTicket handshake message in a resumption handshake replaces cached session's ticket before handshake is finished
SecurityFocus
[security-announce] openSUSE-SU-2014:0213-1: important: Mozilla updates
Oracle Critical Patch Update - July 2014
8pecxstudios.com
Security Advisory SA56767 - Mozilla Firefox / Thunderbird / SeaMonkey Multiple Vulnerabilities - Secunia
[security-announce] openSUSE-SU-2014:0212-1: important: Mozilla Firefox
USN-2119-1: Thunderbird vulnerabilities | Ubuntu
Oracle Critical Patch Update - January 2016
USN-2102-2: Firefox regression | Ubuntu
Debian -- Security Information -- DSA-2858-1 iceweasel
[security-announce] openSUSE-SU-2014:0419-1: important: Mozilla updates
Security Advisory SA56858 - Debian update for iceweasel - Secunia
Oracle Critical Patch Update - January 2015

Oracle Critical Patch Update - January 2015
Full Disclosure: NEW: VMSA-2014-0012 - VMware vSphere product updates address security vulnerabilities
VMSA-2014-0012 | United States
Security Advisory SA56787 - Mozilla Firefox Multiple Vulnerabilities - Secunia
IBM X-Force Exchange
osvdb.org/102876
USN-2102-1: Firefox vulnerabilities | Ubuntu
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

Free CVE JSON API cve.report/api

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