CVE-2013-1740

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

Summary

CVE	CVE-2013-1740
State	PUBLISHED
Assigner	mozilla
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-01-18 22:55:03 UTC
Updated	2026-04-29 01:13:23 UTC
Description	The ssl_Do1stHandshake function in sslsecur.c in libssl in Mozilla Network Security Services (NSS) before 3.15.4, when the

Risk And Classification

Primary CVSS: v2.0 5.8 from nvd@nist.gov

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

EPSS: 0.010010000 probability, percentile 0.771070000 (date 2026-05-03)

Problem Types: CWE-310 | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Medium

Authentication

None

Confidentiality

Partial

Integrity

Partial

Availability

None

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language

Application	Mozilla	Network Security Services	3.11.2	All	All	All
Application	Mozilla	Network Security Services	3.11.3	All	All	All
Application	Mozilla	Network Security Services	3.11.4	All	All	All
Application	Mozilla	Network Security Services	3.11.5	All	All	All
Application	Mozilla	Network Security Services	3.12	All	All	All
Application	Mozilla	Network Security Services	3.12.1	All	All	All
Application	Mozilla	Network Security Services	3.12.10	All	All	All
Application	Mozilla	Network Security Services	3.12.11	All	All	All
Application	Mozilla	Network Security Services	3.12.2	All	All	All
Application	Mozilla	Network Security Services	3.12.3	All	All	All
Application	Mozilla	Network Security Services	3.12.3.1	All	All	All
Application	Mozilla	Network Security Services	3.12.3.2	All	All	All
Application	Mozilla	Network Security Services	3.12.4	All	All	All
Application	Mozilla	Network Security Services	3.12.5	All	All	All
Application	Mozilla	Network Security Services	3.12.6	All	All	All
Application	Mozilla	Network Security Services	3.12.7	All	All	All
Application	Mozilla	Network Security Services	3.12.8	All	All	All
Application	Mozilla	Network Security Services	3.12.9	All	All	All
Application	Mozilla	Network Security Services	3.14	All	All	All
Application	Mozilla	Network Security Services	3.14.1	All	All	All
Application	Mozilla	Network Security Services	3.14.2	All	All	All
Application	Mozilla	Network Security Services	3.14.3	All	All	All
Application	Mozilla	Network Security Services	3.14.4	All	All	All
Application	Mozilla	Network Security Services	3.14.5	All	All	All
Application	Mozilla	Network Security Services	3.15	All	All	All
Application	Mozilla	Network Security Services	3.15.1	All	All	All
Application	Mozilla	Network Security Services	3.15.2	All	All	All
Application	Mozilla	Network Security Services	3.2	All	All	All
Application	Mozilla	Network Security Services	3.2.1	All	All	All
Application	Mozilla	Network Security Services	3.3	All	All	All
Application	Mozilla	Network Security Services	3.3.1	All	All	All
Application	Mozilla	Network Security Services	3.3.2	All	All	All
Application	Mozilla	Network Security Services	3.4	All	All	All
Application	Mozilla	Network Security Services	3.4.1	All	All	All
Application	Mozilla	Network Security Services	3.4.2	All	All	All
Application	Mozilla	Network Security Services	3.5	All	All	All

Application	Mozilla	Network Security Services	3.5	All	All	All
Application	Mozilla	Network Security Services	3.6	All	All	All
Application	Mozilla	Network Security Services	3.6.1	All	All	All
Application	Mozilla	Network Security Services	3.7	All	All	All
Application	Mozilla	Network Security Services	3.7.1	All	All	All
Application	Mozilla	Network Security Services	3.7.2	All	All	All
Application	Mozilla	Network Security Services	3.7.3	All	All	All
Application	Mozilla	Network Security Services	3.7.5	All	All	All
Application	Mozilla	Network Security Services	3.7.7	All	All	All
Application	Mozilla	Network Security Services	3.8	All	All	All
Application	Mozilla	Network Security Services	3.9	All	All	All
Application	Mozilla	Network Security Services	All	All	All	All

Vendor Declared Affected Products

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

References

Reference	Sou
Network Security Services 'ssl_Do1stHandshake()' Function Information Disclosure Vulnerability	af85
Bug 1053725 – CVE-2013-1740 nss: false start PR_Recv information disclosure security issue	af85
498172 – (CVE-2013-1740) <dev-libs/nss-3.15.4: False Start PR_Recv Information Disclosure Security Issue (CVE-2013-1740)	af85
USN-2088-1: NSS vulnerability | Ubuntu	af85
Oracle VM Server for x86 Bulletin - July 2016	af85
Oracle Critical Patch Update - October 2014	af85
SecurityFocus	af85
[security-announce] openSUSE-SU-2014:0213-1: important: Mozilla updates	af85
NSS 3.15.4 release notes - Mozilla | MDN	af85
919877 – (CVE-2013-1740) When false start is enabled, libssl will sometimes return unencrypted, unauthenticated data from PR_Recv	af85
Oracle Critical Patch Update - July 2014	af85
IBM X-Force Exchange	af85
[security-announce] openSUSE-SU-2014:0212-1: important: Mozilla Firefox	af85
Oracle Critical Patch Update - January 2016	af85
Oracle Critical Patch Update - January 2015	af85
Full Disclosure: NEW: VMSA-2014-0012 - VMware vSphere product updates address security vulnerabilities	af85
VMSA-2014-0012 | United States	af85
CVE Program record	CVE

NVD vulnerability detail	NVD

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**