CVE-2014-1492

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

Summary

CVE	CVE-2014-1492
State	PUBLISHED
Assigner	mozilla
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-03-25 13:25:38 UTC
Updated	2026-05-06 22:30:45 UTC
Description	The cert_TestHostName function in lib/certdb/certdb.c in the certificate-checking implementation in Mozilla Network Securit

Risk And Classification

Primary CVSS: v2.0 4.3 from nvd@nist.gov

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

Problem Types: CWE-20 | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Medium

Authentication

None

Confidentiality

None

Integrity

Partial

Availability

None

AV:N/AC:M/Au:N/C:N/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	3.15.3	All	All	All
Application	Mozilla	Network Security Services	3.15.3.1	All	All	All
Application	Mozilla	Network Security Services	3.15.4	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	3.6	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	Source
2016-10 Security Bulletin: CTPView: Multiple vulnerabilities in CTPView - Juniper Networks	af854a3a
[SECURITY] Fedora 19 Update: firefox-29.0-5.fc19	af854a3a
About Secunia Research | Flexera	af854a3a
Gentoo Security	af854a3a
Bug 1079851 – CVE-2014-1492 nss: IDNA hostname matching code does not follow RFC 6125 recommendation (MFSA 2014-45)	af854a3a
MFSA 2014-45: Incorrect IDNA domain name matching for wildcard certificates	af854a3a
Oracle VM Server for x86 Bulletin - July 2016	af854a3a
Debian -- Security Information -- DSA-2994-1 nss	af854a3a
Oracle Critical Patch Update - October 2014	af854a3a
USN-2159-1: NSS vulnerability | Ubuntu	af854a3a
openSUSE-SU-2014:0629-1: moderate: update for seamonkey	af854a3a
Mozilla Network Security Services CVE-2014-1492 Security Bypass Vulnerability	af854a3a
nss: changeset 11063:709d4e597979	af854a3a
About Secunia Research | Flexera	af854a3a
SecurityFocus	af854a3a
Oracle Critical Patch Update - July 2014	af854a3a

USN-2185-1: Firefox vulnerabilities | Ubuntu	af854a3a
NSS 3.16 release notes - Mozilla | MDN	af854a3a
Oracle Critical Patch Update - January 2016	af854a3a
Security Advisory SA60621 - SUSE update for MozillaFirefox and MozillaThunderbird - Secunia	af854a3a
[security-announce] SUSE-SU-2014:0665-1: important: Security update for	af854a3a
openSUSE-SU-2014:0599-1: moderate: update for MozillaFirefox	af854a3a
[security-announce] SUSE-SU-2014:0727-1: important: Security update for	af854a3a
Oracle Critical Patch Update - January 2015	af854a3a
903885 – (CVE-2014-1492) Hostname matching code violates RFC 6125 for IDNA	af854a3a
Full Disclosure: NEW: VMSA-2014-0012 - VMware vSphere product updates address security vulnerabilities	af854a3a
VMSA-2014-0012 | United States	af854a3a
CVE Program record	CVE.OR
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**