



CVE-2015-2721

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

| | |
|------------------------|---|
| CVE | CVE-2015-2721 |
| State | PUBLIC |
| Assigner | security@mozilla.org |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2015-07-06 02:00:00 UTC |
| Updated | 2023-09-12 14:55:00 UTC |
| Description | Mozilla Network Security Services (NSS) before 3.19, as used in Mozilla Firefox before 39.0, Firefox ESR 31.x before 31.8 |

Risk And Classification

Problem Types: CWE-310

NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|------------------|-----------|--------------|---------|--------|---------|----------|
| Operating System | Canonical | Ubuntu Linux | 12.04 | All | All | All |
| Operating System | Canonical | Ubuntu Linux | 14.04 | All | All | All |
| Operating System | Canonical | Ubuntu Linux | 14.10 | All | All | All |
| Operating System | Canonical | Ubuntu Linux | 15.04 | All | All | All |
| Operating System | Canonical | Ubuntu Linux | 12.04 | All | All | All |
| Operating System | Canonical | Ubuntu Linux | 14.04 | All | All | All |
| Operating System | Canonical | Ubuntu Linux | 14.10 | All | All | All |
| Operating System | Canonical | Ubuntu Linux | 15.04 | All | All | All |
| Operating System | Debian | Debian Linux | 7.0 | All | All | All |
| Operating System | Debian | Debian Linux | 8.0 | All | All | All |
| Operating System | Debian | Debian Linux | 7.0 | All | All | All |
| Operating System | Debian | Debian Linux | 8.0 | All | All | All |
| Application | Mozilla | Firefox | All | All | All | All |
| Application | Mozilla | Firefox | All | All | All | All |
| Application | Mozilla | Firefox Esr | 31.0 | All | All | All |
| Application | Mozilla | Firefox Esr | 31.1 | All | All | All |
| Application | Mozilla | Firefox Esr | 31.1.0 | All | All | All |

| | | | | | | |
|------------------|---------|-------------------------------|--------|-----|-----|-----|
| Application | Mozilla | Firefox Esr | 31.1.1 | All | All | All |
| Application | Mozilla | Firefox Esr | 31.2 | All | All | All |
| Application | Mozilla | Firefox Esr | 31.3 | All | All | All |
| Application | Mozilla | Firefox Esr | 31.3.0 | All | All | All |
| Application | Mozilla | Firefox Esr | 31.4 | All | All | All |
| Application | Mozilla | Firefox Esr | 31.5 | All | All | All |
| Application | Mozilla | Firefox Esr | 31.5.1 | All | All | All |
| Application | Mozilla | Firefox Esr | 31.5.2 | All | All | All |
| Application | Mozilla | Firefox Esr | 31.5.3 | All | All | All |
| Application | Mozilla | Firefox Esr | 31.6.0 | All | All | All |
| Application | Mozilla | Firefox Esr | 31.7.0 | All | All | All |
| Application | Mozilla | Firefox Esr | 38.0 | All | All | All |
| Application | Mozilla | Firefox Esr | 31.0 | All | All | All |
| Application | Mozilla | Firefox Esr | 31.1 | All | All | All |
| Application | Mozilla | Firefox Esr | 31.1.0 | All | All | All |
| Application | Mozilla | Firefox Esr | 31.1.1 | All | All | All |
| Application | Mozilla | Firefox Esr | 31.2 | All | All | All |
| Application | Mozilla | Firefox Esr | 31.3 | All | All | All |
| Application | Mozilla | Firefox Esr | 31.3.0 | All | All | All |
| Application | Mozilla | Firefox Esr | 31.4 | All | All | All |
| Application | Mozilla | Firefox Esr | 31.5 | All | All | All |
| Application | Mozilla | Firefox Esr | 31.5.1 | All | All | All |
| Application | Mozilla | Firefox Esr | 31.5.2 | All | All | All |
| Application | Mozilla | Firefox Esr | 31.5.3 | All | All | All |
| Application | Mozilla | Firefox Esr | 31.6.0 | All | All | All |
| Application | Mozilla | Firefox Esr | 31.7.0 | All | All | All |
| Application | Mozilla | Firefox Esr | 38.0 | All | All | All |
| Application | Mozilla | Network Security Services | 3.19 | All | All | All |
| Application | Mozilla | Network Security Services | 3.19 | All | All | All |
| Application | Mozilla | Thunderbird | All | All | All | All |
| Application | Mozilla | Thunderbird | All | All | All | All |
| Operating System | Novell | Suse Linux Enterprise Desktop | 12.0 | All | All | All |
| Operating System | Novell | Suse Linux Enterprise Desktop | 12.0 | All | All | All |
| Operating System | Novell | Suse Linux Enterprise Server | 11 | sp4 | All | All |
| Operating System | Novell | Suse Linux Enterprise Server | 12.0 | All | All | All |

| | | | | | | |
|------------------|--------|--|------|-----|-----|-----|
| Operating System | Novell | Suse Linux Enterprise Server | 11 | sp4 | All | All |
| Operating System | Novell | Suse Linux Enterprise Server | 12.0 | All | All | All |
| Application | Novell | Suse Linux Enterprise Software Development Kit | 12.0 | All | All | All |
| Operating System | Novell | Suse Linux Enterprise Software Development Kit | 12.0 | All | All | All |
| Operating System | Novell | Suse Linux Enterprise Software Development Kit | 12.0 | All | All | All |
| Operating System | Oracle | Solaris | 11.3 | All | All | All |
| Operating System | Oracle | Solaris | 11.3 | All | All | All |
| Operating System | Oracle | Vm Server | 3.2 | All | All | All |
| Operating System | Oracle | Vm Server | 3.2 | All | All | All |

References

Reference

Oracle Solaris Bulletin - April 2016

Oracle Critical Patch Update Advisory - April 2016

[security-announce] openSUSE-SU-2015:1229-1: important: Security update

miTLS - A verified reference implementation of TLS

USN-2672-1: NSS vulnerabilities | Ubuntu

Oracle Critical Patch Update - July 2016

Oracle July 2016 Critical Patch Update Multiple Vulnerabilities

Debian -- Security Information -- DSA-3336-1 nss

[security-announce] SUSE-SU-2015:1268-1: important: Security update for

USN-2656-2: Firefox vulnerabilities | Ubuntu

[security-announce] openSUSE-SU-2015:1266-1: important: Mozilla (Firefox

USN-2673-1: Thunderbird vulnerabilities | Ubuntu

Mozilla Firefox Multiple Flaws Let Remote Users Execute Arbitrary Code, Obtain Potentially Sensitive Information, Bypass Security Restriction

Oracle Solaris Third Party Bulletin - October 2015

[security-announce] SUSE-SU-2015:1269-1: important: Security update for

Mozilla Network Security Services CVE-2015-2721 Security Bypass Vulnerability

Oracle VM Server for x86 Bulletin - July 2016

1086145 – (CVE-2015-2721) NSS incorrectly permits skipping of ServerKeyExchange

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


Debian -- Security Information -- DSA-3324-1 icedove

[security-announce] SUSE-SU-2015:1449-1: important: Security update for

USN-2656-1: Firefox vulnerabilities | Ubuntu

NSS 3.19 release notes - Mozilla | MDN

NSS incorrectly permits skipping of ServerKeyExchange — Mozilla

| |
|---|
| Red Hat Customer Portal |
| Mozilla Products: Multiple vulnerabilities (GLSA 201512-10) — Gentoo Security |
| Red Hat Customer Portal |
| Mozilla Thunderbird Multiple Flaws Let Remote Users Execute Arbitrary Code, Obtain Potentially Sensitive Information, and Bypass Security F |
| Mozilla Firefox/Thunderbird Multiple Security Vulnerabilities |
| CVE Program record |
| NVD vulnerability detail |
|  |
| No vendor comments have been submitted for this CVE. |
| Legacy QID Mappings |
| 710518 Gentoo Linux Mozilla Network Security Service (NSS) Multiple Vulnerabilities (GLSA 201701-46) |

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)