

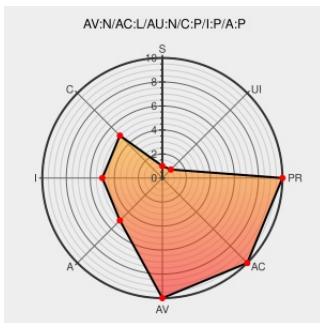


CVE-2015-7181

Published on: 11/04/2015 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:12 PM UTC

CVE-2015-7181

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Firefox](#) from [Mozilla](#) contain the following vulnerability:

The `sec_asn1d_parse_leaf` function in Mozilla Network Security Services (NSS) before 3.19.2.1 and 3.20.x before 3.20.1, as used in Firefox before 42.0 and Firefox ESR 38.x before 38.4 and other products, improperly restricts access to an unspecified data structure, which allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via crafted OCTET STRING data, related to a "use-after-poison" issue.

CVE-2015-7181 has been assigned by [m](#) security@mozilla.org to track the vulnerability

CVSS2 Score: **7.5 - HIGH**

Access
Vector

NETWORK

Access
Complexity

LOW

Authentication

NONE

Confidentiality
Impact

PARTIAL

Integrity
Impact

PARTIAL

Availability
Impact

PARTIAL

CVE References

Description

Tags

Link

Oracle Solaris Bulletin - April 2016

[www.oracle.com](#)
[text/html](#)

[CONFIRM](#)
[www.oracle.com/technetwork/topics/security/bulletinapr2016-2952098.html](#)

Oracle Critical Patch Update Advisory - April 2016

[www.oracle.com](#)
[text/html](#)

[CONFIRM](#) [www.oracle.com/technetwork/security-advisory/cpuapr2016v3-2985753.html](#)

Mozilla Network Security Services Memory Corruption and Heap Buffer Overflow Vulnerabilities

[cve.report \(archive\)](#)
[text/html](#)

[BID 77416](#)

Oracle Critical Patch Update - July 2016

[www.oracle.com](#)

[CONFIRM](#) [www.oracle.com/technetwork/security-](#)

	text/html	advisory/cpujul2016-2881720.html
[security-announce] SUSE-SU-2015:1978-1: important: Security update for	lists.opensuse.org text/html	 SUSE SUSE-SU-2015:1978
Oracle July 2016 Critical Patch Update Multiple Vulnerabilities	cve.report (archive) text/html	 BID 91787
1192028 - (CVE-2015-7181) ASan: use-after-poison in sec_asn1d_parse_leaf()	bugzilla.mozilla.org text/html	 CONFIRM bugzilla.mozilla.org/show_bug.cgi?id=1192028
openSUSE-SU-2015:2245-1: moderate: Security update for Mozilla Thunderbi	lists.opensuse.org text/html	 SUSE openSUSE-SU-2015:2245
openSUSE-SU-2015:2229-1: moderate: Security update for MozillaThunderbir	lists.opensuse.org text/html	 SUSE openSUSE-SU-2015:2229
USN-2791-1: NSS vulnerabilities Ubuntu	www.ubuntu.com text/html	 UBUNTU USN-2791-1
Mozilla Products: Multiple vulnerabilities (GLSA 201605-06) — Gentoo security	security.gentoo.org text/html	 GENTOO GLSA-201605-06
NSS 3.20.1 release notes - Mozilla MDN	Vendor Advisory developer.mozilla.org text/html	 CONFIRM developer.mozilla.org/en-US/docs/Mozilla/Projects/NSS/NSS_3.20.1_release_notes
[security-announce] SUSE-SU-2015:1981-1: important: Security update for	lists.opensuse.org text/html	 SUSE SUSE-SU-2015:1981
[security-announce] SUSE-SU-2015:1926-1: important: Security update for	lists.opensuse.org text/html	 SUSE SUSE-SU-2015:1926
NSS and NSPR memory corruption issues — Mozilla	Vendor Advisory www.mozilla.org text/html	 CONFIRM www.mozilla.org/security/announce/2015/mfsa2015-133.html
Red Hat Customer Portal	web.archive.org text/html Inactive Link Not Archived	 REDHAT RHSA-2015:1981
Debian -- Security Information -- DSA-3688-1 nss	www.debian.org Deprecated Link text/html	 DEBIAN DSA-3688
The Slackware Linux Project: Slackware Security Advisories	www.slackware.com text/html	 SLACKWARE SSA:2015-310-02
Oracle VM Server for x86 Bulletin - July 2016	web.archive.org text/html Inactive Link Not Archived	 CONFIRM www.oracle.com/technetwork/topics/security/ovmbulletinjul2016-3090546.html
Debian -- Security Information -- DSA-3393-1 iceweasel	www.debian.org Deprecated Link text/html	 DEBIAN DSA-3393
USN-2819-1: Thunderbird vulnerabilities Ubuntu	www.ubuntu.com text/html	 UBUNTU USN-2819-1
Debian -- Security Information -- DSA-3410-1 icedove	www.debian.org Deprecated Link text/html	 DEBIAN DSA-3410
Oracle Linux Bulletin - October 2015	www.oracle.com text/html	 CONFIRM www.oracle.com/technetwork/topics/security/linuxbulletinoct2015-2719645.html
Mozilla Firefox Multiple Flaws Let Remote Users Execute Arbitrary Code, Obtain	www.securitytracker.com text/html	 SECTRAK 1034069

Users Execute Arbitrary Code, Obtain Potentially Sensitive Information, Bypass Security Restrictions, and Conduct Cross-Site Scripting Attacks - SecurityTracker	text/html	
Red Hat Customer Portal	web.archive.org text/html Inactive Link Not Archived	 REDHAT RHSA-2015:1980
Mozilla Products: Multiple vulnerabilities (GLSA 201512-10) — Gentoo Security	security.gentoo.org text/html	 GENTOO GLSA-201512-10
Slackware Security Advisory - mozilla-nss Updates ≈ Packet Storm	packetstormsecurity.com text/html	 MISC packetstormsecurity.com/files/134268/Slackware-Security-Advisory-mozilla-nss-Updates.html
NSS 3.19.4 release notes - Mozilla MDN	Vendor Advisory developer.mozilla.org text/html	 CONFIRM developer.mozilla.org/en-US/docs/Mozilla/Projects/NSS/NSS_3.19.4_release_notes
Broadcom Support Portal	bto.bluecoat.com text/html	 CONFIRM bto.bluecoat.com/security-advisory/sa119
[security-announce] openSUSE-SU-2015:1942-1: important: Security update	lists.opensuse.org text/html	 SUSE openSUSE-SU-2015:1942
[security-announce] SUSE-SU-2015:2081-1: important: Security update for	lists.opensuse.org text/html	 SUSE SUSE-SU-2015:2081
Oracle Critical Patch Update - October 2017	www.oracle.com text/html	 CONFIRM www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html
NSS 3.19.2.1 release notes - Mozilla MDN	Vendor Advisory developer.mozilla.org text/html	 CONFIRM developer.mozilla.org/en-US/docs/Mozilla/Projects/NSS/NSS_3.19.2.1_release_notes
USN-2785-1: Firefox vulnerabilities Ubuntu	www.ubuntu.com text/html	 UBUNTU USN-2785-1

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
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	38.0	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	Network Security Services	3.20.0	All	All	All
Application	Mozilla	Network Security Services	3.20.0	All	All	All
Application	Mozilla	Network Security Services	All	All	All	All
cpe:2.3:a:mozilla:firefox:*.***.***.***:						
cpe:2.3:a:mozilla:firefox_esr:38.0:*.***.***.***:						
cpe:2.3:a:mozilla:firefox_esr:38.0.1:*.***.***.***:						
cpe:2.3:a:mozilla:firefox_esr:38.0.5:*.***.***.***:						
cpe:2.3:a:mozilla:firefox_esr:38.1.0:*.***.***.***:						
cpe:2.3:a:mozilla:firefox_esr:38.1.1:*.***.***.***:						
cpe:2.3:a:mozilla:firefox_esr:38.2.0:*.***.***.***:						
cpe:2.3:a:mozilla:firefox_esr:38.2.1:*.***.***.***:						
cpe:2.3:a:mozilla:firefox_esr:38.3.0:*.***.***.***:						
cpe:2.3:a:mozilla:firefox_esr:38.0:*.***.***.***:						
cpe:2.3:a:mozilla:firefox_esr:38.0.1:*.***.***.***:						
cpe:2.3:a:mozilla:firefox_esr:38.0.5:*.***.***.***:						
cpe:2.3:a:mozilla:firefox_esr:38.1.0:*.***.***.***:						
cpe:2.3:a:mozilla:firefox_esr:38.1.1:*.***.***.***:						
cpe:2.3:a:mozilla:firefox_esr:38.2.0:*.***.***.***:						
cpe:2.3:a:mozilla:firefox_esr:38.2.1:*.***.***.***:						
cpe:2.3:a:mozilla:firefox_esr:38.3.0:*.***.***.***:						
cpe:2.3:a:mozilla:network_security_services:3.20.0:*.***.***.***:						
cpe:2.3:a:mozilla:network_security_services:3.20.0:*.***.***.***:						

cpe:2.3:a:mozilla:network_security_services:*****:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID→](#)

© [CVE.report](#) 2023   |

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](#)