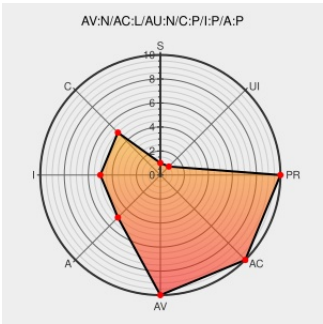
CVE-2014-1569

Published on: 12/15/2014 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:47 PM UTC

CVE-2014-1569

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Network Security Services from Mozilla contain the following vulnerability:

The definite_length_decoder function in lib/util/quickder.c in Mozilla Network Security Services (NSS) before 3.16.2.4 and 3.17.x before 3.17.3 does not ensure that the DER encoding of an ASN.1 length is properly formed, which allows remote attackers to conduct data-smuggling attacks by using a long byte sequence for an encoding, as demonstrated by the SEC_QuickDERDecodeItem function's improper handling of an arbitrary-length encoding of 0x00.

CVE-2014-1569 has been assigned by security@mozilla.org to track the vulnerability

CVSS2 Score: 7.5 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	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
Hardware-Enabled Security	Exploit www.intelsecurity.com application/pdf	MISC www.intelsecurity.com/resources/wp-berserk-analysis-part-1.pdf
[security-announce] SUSE-SU-2015:0171-1: important: Security update for	lists.opensuse.org text/html	SUSE SUSE-SU-2015:0171
[security-announce] SUSE-	lists.opensuse.org	SUSE SUSE-SU-2015:0173

SU-2015:0173-1: important: Security update for	text/html	
1064670 – (CVE-2014-1569) ASN.1 DER decoding of lengths is too permissive, allowing undetected smuggling of arbitrary data	Exploit bugzilla.mozilla.org text/html	CONFIRM bugzilla.mozilla.org/show_bug.cgi?id=1064670
NSS 3.17.3 release notes - Mozilla | MDN	Vendor Advisory developer.mozilla.org text/html	CONFIRM developer.mozilla.org/en-US/docs/Mozilla/Projects/NSS/NSS_3.17.3_release_notes
Oracle Critical Patch Update - October 2015	www.oracle.com text/html	CONFIRM www.oracle.com/technetwork/topics/security/cpuoct2015-2367953.html
Oracle Critical Patch Update - July 2015	www.oracle.com text/html	CONFIRM www.oracle.com/technetwork/topics/security/cpujul2015-2367936.html
benmmurphy comments on RSA Signature Forgery in NSS	Exploit www.reddit.com text/html	MISC www.reddit.com/r/netsec/comments/2hd1m8/rsa_signature_forgery_in_nss/cksnr02
[security-announce] openSUSE-SU-2015:0404-1: important: Security update	lists.opensuse.org text/html	SUSE openSUSE-SU-2015:0404
[security-announce] openSUSE-SU-2015:0138-1: important: Firefox update t	lists.opensuse.org text/html	SUSE openSUSE-SU-2015:0138
ImperialViolet - PKCS#1 signature validation	Exploit www.imperialviolet.org text/html	MISC www.imperialviolet.org/2014/09/26/pkcs1.html
Debian -- Security Information -- DSA-3186-1 nss	www.debian.org Depreciated Link text/html	DEBIAN DSA-3186
[security-announce] SUSE-SU-2015:0180-1: important: Security update for	lists.opensuse.org text/html	SUSE SUSE-SU-2015:0180
Oracle Communications Applications Flaws Let Remote Users Gain Elevated Privileges and Partially Access Data, Modify Data, and Deny Service - SecurityTracker	www.securitytracker.com text/html	SECTRACK 1032909

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language

Application	Mozilla	Network Security Services	3.16.2.0	All	All	All
Application	Mozilla	Network Security Services	3.16.2.1	All	All	All
Application	Mozilla	Network Security Services	3.16.2.2	All	All	All
Application	Mozilla	Network Security Services	3.17.0	All	All	All
Application	Mozilla	Network Security Services	3.17.1	All	All	All
Application	Mozilla	Network Security Services	3.17.2	All	All	All
Application	Mozilla	Network Security Services	3.16.2.0	All	All	All
Application	Mozilla	Network Security Services	3.16.2.1	All	All	All
Application	Mozilla	Network Security Services	3.16.2.2	All	All	All
Application	Mozilla	Network Security Services	3.17.0	All	All	All
Application	Mozilla	Network Security Services	3.17.1	All	All	All
Application	Mozilla	Network Security Services	3.17.2	All	All	All
Application	Mozilla	Network Security Services	All	All	All	All

cpe:2.3:a:mozilla:network_security_services:3.16.2.0:*:*:*:*:*:*:*:

cpe:2.3:a:mozilla:network_security_services:3.16.2.1:*:*:*:*:*:*:*:

cpe:2.3:a:mozilla:network_security_services:3.16.2.2:*:*:*:*:*:*:*:

cpe:2.3:a:mozilla:network_security_services:3.17.0:*:*:*:*:*:*:*:

cpe:2.3:a:mozilla:network_security_services:3.17.1:*:*:*:*:*:*:*:

cpe:2.3:a:mozilla:network_security_services:3.17.2:*:*:*:*:*:*:*:

cpe:2.3:a:mozilla:network_security_services:3.16.2.0:*:*:*:*:*:*:*:

cpe:2.3:a:mozilla:network_security_services:3.16.2.1:*:*:*:*:*:*:*:

cpe:2.3:a:mozilla:network_security_services:3.16.2.2:*:*:*:*:*:*:*:

cpe:2.3:a:mozilla:network_security_services:3.17.0:*:*:*:*:*:*:*:

cpe:2.3:a:mozilla:network_security_services:3.17.1:*:*:*:*:*:*:*:

cpe:2.3:a:mozilla:network_security_services:3.17.2:*:*:*:*:*:*:*:

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

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

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