



# 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 [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](#)

Hardware-Enabled Security

[Exploit](#)  
[www.intelsecurity.com](#)  
[application/pdf](#)

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

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](mailto: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 | 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.*:*:*:*:*:*:
```

```
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→

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](#)