



# CVE-2015-8659

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2015-8659
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2016-01-12 19:59:00 UTC
<b>Updated</b>	2019-03-08 16:06:00 UTC
<b>Description</b>	The idle stream handling in nghttp2 before 1.6.0 allows attackers to have unspecified impact via unknown vectors, aka a he

## Risk And Classification

**Problem Types:** CWE-119

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Apple</a>	<a href="#">Iphone Os</a>	All	All	All	All
Operating System	<a href="#">Apple</a>	<a href="#">Mac Os X</a>	All	All	All	All
Operating System	<a href="#">Apple</a>	<a href="#">Tvos</a>	All	All	All	All
Operating System	<a href="#">Apple</a>	<a href="#">Watchos</a>	All	All	All	All
Application	<a href="#">Nghttp2</a>	<a href="#">Nghttp2</a>	All	All	All	All

## References

### Reference

- [APPLE-SA-2016-03-21-2 watchOS 2.2](#)
- [APPLE-SA-2016-03-21-5 OS X El Capitan 10.11.4 and Security Update 2016-002](#)
- [Nghttp2 v1.6.0 - nghttp2.org](#)
- [APPLE-SA-2016-03-21-3 tvOS 9.2](#)
- [oss-security - Re: Use after free in nghttp2](#)
- [\[SECURITY\] Fedora 22 Update: nghttp2-1.6.0-1.fc22](#)
- [About the security content of watchOS 2.2 - Apple Support](#)
- [About the security content of iOS 9.3 - Apple Support](#)
- [nghttp2: Heap-use-after-free \(GLSA 201612-06\) — Gentoo security](#)

oss-security - Use after free in nghttp2

[SECURITY] Fedora 23 Update: nghttp2-1.6.0-1.fc23

APPLE-SA-2016-03-21-1 iOS 9.3

Apple iOS Multiple Flaws Let Remote Users Execute Arbitrary Code and Let Remote and Local Users Obtain Potentially Sensitive Information

About the security content of OS X El Capitan v10.11.4 and Security Update 2016-002 - Apple Support

About the security content of tvOS 9.2 - Apple Support

CVE Program record

NVD vulnerability detail



No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [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](#)