CVE-2015-8659

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2015-8659
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2016-01-12 19:59:00 UTC
Updated	2019-03-08 16:06:00 UTC
Description	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	Apple	Iphone Os	All	All	All	All
Operating System	Apple	Mac Os X	All	All	All	All
Operating System	Apple	Tvos	All	All	All	All
Operating System	Apple	Watchos	All	All	All	All
Application	Nghttp2	Nghttp2	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.