



CVE-2018-16844

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

Summary

CVE	CVE-2018-16844
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-11-07 14:29:00 UTC
Updated	2022-02-22 19:27:00 UTC
Description	nginx before versions 1.15.6 and 1.14.1 has a vulnerability in the implementation of HTTP/2 that can allow for excessive CF

Risk And Classification

Problem Types: CWE-400

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Apple	Xcode	All	All	All	All
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Canonical	Ubuntu Linux	18.04	All	All	All
Operating System	Canonical	Ubuntu Linux	18.10	All	All	All
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Canonical	Ubuntu Linux	18.04	All	All	All
Operating System	Canonical	Ubuntu Linux	18.10	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Application	F5	Nginx	All	All	All	All
Application	Nginx	Nginx	All	All	All	All
Application	Nginx	Nginx	All	All	All	All

References

Reference	Source	Link
-----------	--------	------

Red Hat Customer Portal	REDHAT	access.red
[nginx-announce] nginx security advisory (CVE-2018-16843, CVE-2018-16844)	MISC	mailman.ng
Full Disclosure: APPLE-SA-2021-09-20-4 Xcode 13	FULLDISC	seclists.org
Red Hat Customer Portal	REDHAT	access.red
nginx HTTP/2 Processing Bugs Lets Remote Users Deny Service - SecurityTracker	SECTRACK	www.secur
[security-announce] openSUSE-SU-2019:2120-1: important: Security update	SUSE	lists.opensu
About the security content of Xcode 13 - Apple Support	CONFIRM	support.ap
USN-3812-1: nginx vulnerabilities Ubuntu security notices	UBUNTU	usn.ubuntu
Debian -- Security Information -- DSA-4335-1 nginx	DEBIAN	www.debia
1644510 – (CVE-2018-16844) CVE-2018-16844 nginx: Excessive CPU usage via flaw in HTTP/2 implementation	CONFIRM	bugzilla.rec
nginx Multiple Denial of Service Vulnerabilities	BID	www.secur
CVE Program record	CVE.ORG	www.cve.o
NVD vulnerability detail	NVD	nvd.nist.go

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[375873](#) Apple Xcode Prior to 13 Vulnerability (HT212818)

[500426](#) Alpine Linux Security Update for nginx

[504185](#) Alpine Linux Security Update for nginx

© [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](#)