



# CVE-2018-16843

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

## Summary

<b>CVE</b>	CVE-2018-16843
<b>State</b>	PUBLIC
<b>Assigner</b>	secalert@redhat.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2018-11-07 14:29:00 UTC
<b>Updated</b>	2022-02-22 19:27:00 UTC
<b>Description</b>	nginx before versions 1.15.6 and 1.14.1 has a vulnerability in the implementation of HTTP/2 that can allow for excessive me

## Risk And Classification

**Problem Types:** CWE-400

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Apple</a>	<a href="#">Xcode</a>	All	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	14.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	16.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	18.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	18.10	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	14.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	16.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	18.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	18.10	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	9.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	9.0	All	All	All
Application	<a href="#">F5</a>	<a href="#">Nginx</a>	All	All	All	All
Application	<a href="#">Nginx</a>	<a href="#">Nginx</a>	All	All	All	All
Application	<a href="#">Nginx</a>	<a href="#">Nginx</a>	All	All	All	All
Operating System	<a href="#">Opensuse</a>	<a href="#">Leap</a>	15.1	All	All	All
Operating System	<a href="#">Opensuse</a>	<a href="#">Leap</a>	15.1	All	All	All

## References

Reference	Source	L
Red Hat Customer Portal	REDHAT	e
[nginx-announce] nginx security advisory (CVE-2018-16843, CVE-2018-16844)	MISC	r
Full Disclosure: APPLE-SA-2021-09-20-4 Xcode 13	FULLDISC	s
Red Hat Customer Portal	REDHAT	e
1644511 – (CVE-2018-16843) CVE-2018-16843 nginx: Excessive memory consumption via flaw in HTTP/2 implementation	CONFIRM	t
Red Hat Customer Portal	REDHAT	e
nginx HTTP/2 Processing Bugs Lets Remote Users Deny Service - SecurityTracker	SECTRACK	v
[security-announce] openSUSE-SU-2019:2120-1: important: Security update	SUSE	li
About the security content of Xcode 13 - Apple Support	CONFIRM	s
USN-3812-1: nginx vulnerabilities   Ubuntu security notices	UBUNTU	u
Debian -- Security Information -- DSA-4335-1 nginx	DEBIAN	v
nginx Multiple Denial of Service Vulnerabilities	BID	v
CVE Program record	CVE.ORG	v
NVD vulnerability detail	NVD	r

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](#)