



# CVE-2016-0747

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

## Summary

<b>CVE</b>	CVE-2016-0747
<b>State</b>	PUBLIC
<b>Assigner</b>	secalert@redhat.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2016-02-15 19:59:00 UTC
<b>Updated</b>	2021-12-16 18:43:00 UTC
<b>Description</b>	The resolver in nginx before 1.8.1 and 1.9.x before 1.9.10 does not properly limit CNAME resolution, which allows remote a

## 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>	15.10	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>	15.10	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	7.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	8.0	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>	7.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	8.0	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>	42.1	All	All	All
Operating System	<a href="#">Opensuse</a>	<a href="#">Leap</a>	42.1	All	All	All

References			
Reference	Source	Link	Tags
openSUSE-SU-2016:0371-1: moderate: Security update for nginx	SUSE	<a href="https://lists.opensuse.org">lists.opensuse.org</a>	Mailing
Bug 1302589 – CVE-2016-0747 nginx: Insufficient limits of CNAME resolution in resolver	CONFIRM	<a href="https://bugzilla.redhat.com">bugzilla.redhat.com</a>	Issue T
Debian -- Security Information -- DSA-3473-1 nginx	DEBIAN	<a href="http://www.debian.org">www.debian.org</a>	Third P
Full Disclosure: APPLE-SA-2021-09-20-4 Xcode 13	FULLDISC	<a href="https://seclists.org">seclists.org</a>	
nginx DNS Processing Flaws Let Remote Users Deny Service - SecurityTracker	SECTRACK	<a href="http://www.securitytracker.com">www.securitytracker.com</a>	Third P
nginx: Multiple vulnerabilities (GLSA 201606-06) — Gentoo security	GENTOO	<a href="https://security.gentoo.org">security.gentoo.org</a>	Third P
Red Hat Customer Portal	REDHAT	<a href="https://access.redhat.com">access.redhat.com</a>	Third P
USN-2892-1: nginx vulnerabilities   Ubuntu	UBUNTU	<a href="http://www.ubuntu.com">www.ubuntu.com</a>	Third P
About the security content of Xcode 13 - Apple Support	CONFIRM	<a href="https://support.apple.com">support.apple.com</a>	
nginx security advisory (CVE-2016-0742, CVE-2016-0746, CVE-2016-0747)	MLIST	<a href="https://mailman.nginx.org">mailman.nginx.org</a>	Vendor
Broadcom Support Portal	CONFIRM	<a href="https://bto.bluecoat.com">bto.bluecoat.com</a>	Third P
CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>	canonic
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	canonic

No vendor comments have been submitted for this CVE.

Legacy QID Mappings
<a href="#">375873</a> Apple Xcode Prior to 13 Vulnerability (HT212818)

© 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](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org/cve). This site includes MITRE data granted under the following [license](#).

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)