



CVE-2019-20372

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

Summary

CVE	CVE-2019-20372
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-01-09 21:15:00 UTC
Updated	2022-04-06 16:10:00 UTC
Description	NGINX before 1.17.7, with certain error_page configurations, allows HTTP request smuggling, as demonstrated by the ability to smuggle a request into the error_page configuration.

Risk And Classification

Problem Types: CWE-444

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
Application	F5	Nginx	All	All	All	All
Application	Netapp	Cloud Backup	-	All	All	All
Application	Nginx	Nginx	All	All	All	All
Application	Nginx	Nginx	All	All	All	All
Operating System	Opensuse	Leap	15.1	All	All	All

References

Reference	Source	Link
Duo Network Gateway - Release Notes Duo Security	MISC	duo.com
Use a named location for authSignURL by aledbf · Pull Request #4859 · kubernetes/ingress-nginx · GitHub	MISC	github.com
Full Disclosure: APPLE-SA-2021-09-20-4 Xcode 13	FULLDISC	seclists.org
CVE-2019-20372 NGINX vulnerability in NetApp Products NetApp Product Security	CONFIRM	security.netapp.co
nginx.org/en/CHANGES	MISC	nginx.org
bertjwregeer.keybase.pub/2019-12-10%20-%20error_page%20request%20smuggling.pdf	MISC	bertjwregeer.keyba
About the security content of Xcode 13 - Apple Support	CONFIRM	support.apple.com

Discard request body when redirecting to a URL via error_page. · nginx/nginx@c1be55f · GitHub	CONFIRM	github.com
USN-4235-1: nginx vulnerability Ubuntu security notices Ubuntu	UBUNTU	usn.ubuntu.com
[security-announce] openSUSE-SU-2020:0204-1: moderate: Security update f	SUSE	lists.opensuse.org
USN-4235-2: nginx vulnerability Ubuntu security notices Ubuntu	UBUNTU	usn.ubuntu.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

14013 Ansible Tower Security Update 3.8.1 Multiple Vulnerabilities
356167 Amazon Linux Security Advisory for nginx : ALASNGINX1-2023-004
375873 Apple Xcode Prior to 13 Vulnerability (HT212818)
500428 Alpine Linux Security Update for nginx
504187 Alpine Linux Security Update for nginx
900179 CBL-Mariner Linux Security Update for nginx 1.16.1
903254 Common Base Linux Mariner (CBL-Mariner) Security Update for nginx (2699)
940220 AlmaLinux Security Update for nginx:1.16 (ALSA-2020:5495)

© [CVE.report](https://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