



CVE-2022-23959

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

Summary

CVE	CVE-2022-23959
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-01-26 01:15:00 UTC
Updated	2023-11-07 03:44:00 UTC
Description	In Varnish Cache before 6.6.2 and 7.x before 7.0.2, Varnish Cache 6.0 LTS before 6.0.10, and and Varnish Enterprise (Cac

Risk And Classification

Problem Types: CWE-444

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	10.0	All	All	All
Operating System	Debian	Debian Linux	11.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Fedoraproject	Fedora	35	All	All	All
Application	Varnish-software	Varnish Cache	All	All	All	All
Application	Varnish-software	Varnish Cache	All	All	All	All
Application	Varnish-software	Varnish Cache	All	All	All	All
Application	Varnish-software	Varnish Cache	4.1	All	All	All
Application	Varnish-software	Varnish Cache	All	All	All	All
Application	Varnish-software	Varnish Cache Plus	All	All	All	All
Application	Varnish Cache Project	Varnish Cache	All	All	All	All

References

Reference	Source	Link
[SECURITY] [DLA 2920-1] varnish security update	MLIST	lists.debian.org
[SECURITY] Fedora 35 Update: varnish-6.6.2-2.fc35 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org
Varnish HTTP/1 Request Smuggling - Varnish Software Documentation	MISC	docs.varnish-software.com

Debian -- Security Information -- DSA-5088-1 varnish	DEBIAN	www.debian.org
VSV00008 Varnish HTTP/1 Request Smuggling Vulnerability — Varnish HTTP Cache	MISC	varnish-cache.org
[SECURITY] Fedora 35 Update: varnish-6.6.2-2.fc35 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org
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

- [159626](#) Oracle Enterprise Linux Security Update for varnish:6 (ELSA-2022-0418)
- [179072](#) Debian Security Update for varnish (DLA 2920-1)
- [179098](#) Debian Security Update for varnish (DSA 5088-1)
- [182438](#) Debian Security Update for varnish (CVE-2022-23959)
- [198827](#) Ubuntu Security Notification for Varnish Cache Vulnerabilities (USN-5474-1)
- [240061](#) Red Hat Update for varnish:6 (RHSA-2022:0418)
- [240063](#) Red Hat Update for varnish:6 (RHSA-2022:0422)
- [240064](#) Red Hat Update for varnish:6 (RHSA-2022:0421)
- [240365](#) Red Hat Update for rh-varnish6-varnish (RHSA-2022:4745)
- [240438](#) Red Hat Update for varnish:6 (RHSA-2022:0420)
- [282392](#) Fedora Security Update for varnish (FEDORA-2022-2f14ec7663)
- [354047](#) Amazon Linux Security Advisory for varnish : ALAS-2022-1632
- [376890](#) Alibaba Cloud Linux Security Update for varnish:6 (ALINUX3-SA-2022:0024)
- [500720](#) Alpine Linux Security Update for varnish
- [501789](#) Alpine Linux Security Update for varnish
- [502036](#) Alpine Linux Security Update for varnish
- [504494](#) Alpine Linux Security Update for varnish
- [690775](#) Free Berkeley Software Distribution (FreeBSD) Security Update for varnish (b0c83e1a-8153-11ec-84f9-641c67a117d8)
- [940449](#) AlmaLinux Security Update for varnish:6 (ALSA-2022:0418)
- [960809](#) Rocky Linux Security Update for varnish:6 (RLSA-2022:0418)

© [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](#)