



CVE-2013-4484

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

Summary

CVE	CVE-2013-4484
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2013-11-01 02:55:00 UTC
Updated	2022-08-02 16:29:00 UTC
Description	Varnish before 3.0.5 allows remote attackers to cause a denial of service (child-process crash and temporary caching outag

Risk And Classification

Problem Types: CWE-119

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Varnish-cache	Varnish	2.0.0	All	All	All
Application	Varnish-cache	Varnish	2.0.1	All	All	All
Application	Varnish-cache	Varnish	2.0.2	All	All	All
Application	Varnish-cache	Varnish	2.0.3	All	All	All
Application	Varnish-cache	Varnish	2.0.4	All	All	All
Application	Varnish-cache	Varnish	2.0.5	All	All	All
Application	Varnish-cache	Varnish	2.0.6	All	All	All
Application	Varnish-cache	Varnish	2.1.0	All	All	All
Application	Varnish-cache	Varnish	2.1.1	All	All	All
Application	Varnish-cache	Varnish	2.1.2	All	All	All
Application	Varnish-cache	Varnish	2.1.3	All	All	All
Application	Varnish-cache	Varnish	2.1.4	All	All	All
Application	Varnish-cache	Varnish	2.1.5	All	All	All
Application	Varnish-cache	Varnish	3.0.0	All	All	All
Application	Varnish-cache	Varnish	3.0.0	beta1	All	All
Application	Varnish-cache	Varnish	3.0.0	beta2	All	All
Application	Varnish-cache	Varnish	3.0.1	All	All	All

Application	Varnish-cache	Varnish	3.0.2	All	All	All
Application	Varnish-cache	Varnish	3.0.3	All	All	All
Application	Varnish-cache	Varnish	2.0.0	All	All	All
Application	Varnish-cache	Varnish	2.0.1	All	All	All
Application	Varnish-cache	Varnish	2.0.2	All	All	All
Application	Varnish-cache	Varnish	2.0.3	All	All	All
Application	Varnish-cache	Varnish	2.0.4	All	All	All
Application	Varnish-cache	Varnish	2.0.5	All	All	All
Application	Varnish-cache	Varnish	2.0.6	All	All	All
Application	Varnish-cache	Varnish	2.1.0	All	All	All
Application	Varnish-cache	Varnish	2.1.1	All	All	All
Application	Varnish-cache	Varnish	2.1.2	All	All	All
Application	Varnish-cache	Varnish	2.1.3	All	All	All
Application	Varnish-cache	Varnish	2.1.4	All	All	All
Application	Varnish-cache	Varnish	2.1.5	All	All	All
Application	Varnish-cache	Varnish	3.0.0	All	All	All
Application	Varnish-cache	Varnish	3.0.0	beta1	All	All
Application	Varnish-cache	Varnish	3.0.0	beta2	All	All
Application	Varnish-cache	Varnish	3.0.1	All	All	All
Application	Varnish-cache	Varnish	3.0.2	All	All	All
Application	Varnish-cache	Varnish	3.0.3	All	All	All
Application	Varnish-cache	Varnish	All	All	All	All
Application	Varnish-cache	Varnish Cache	2.0.1	All	All	All
Application	Varnish-cache	Varnish Cache	2.0.2	All	All	All
Application	Varnish-cache	Varnish Cache	2.0.3	All	All	All
Application	Varnish-cache	Varnish Cache	2.0.4	All	All	All
Application	Varnish-cache	Varnish Cache	2.0.5	All	All	All
Application	Varnish-cache	Varnish Cache	2.0.6	All	All	All
Application	Varnish-cache	Varnish Cache	2.1.0	All	All	All
Application	Varnish-cache	Varnish Cache	2.1.1	All	All	All
Application	Varnish-cache	Varnish Cache	2.1.2	All	All	All
Application	Varnish-cache	Varnish Cache	2.1.3	All	All	All
Application	Varnish-cache	Varnish Cache	2.1.4	All	All	All
Application	Varnish-cache	Varnish Cache	2.1.5	All	All	All
Application	Varnish-cache	Varnish Cache	3.0.0	All	All	All

Application	Varnish-cache	Varnish Cache	3.0.0	beta1	All	All
Application	Varnish-cache	Varnish Cache	3.0.0	beta2	All	All
Application	Varnish-cache	Varnish Cache	3.0.1	All	All	All
Application	Varnish-cache	Varnish Cache	3.0.2	All	All	All
Application	Varnish-cache	Varnish Cache	3.0.3	All	All	All
Application	Varnish-cache	Varnish Cache	All	All	All	All
Application	Varnish Cache Project	Varnish Cache	2.0.1	All	All	All
Application	Varnish Cache Project	Varnish Cache	2.0.2	All	All	All
Application	Varnish Cache Project	Varnish Cache	2.0.3	All	All	All
Application	Varnish Cache Project	Varnish Cache	2.0.4	All	All	All
Application	Varnish Cache Project	Varnish Cache	2.0.5	All	All	All
Application	Varnish Cache Project	Varnish Cache	2.0.6	All	All	All
Application	Varnish Cache Project	Varnish Cache	2.1.0	All	All	All
Application	Varnish Cache Project	Varnish Cache	2.1.1	All	All	All
Application	Varnish Cache Project	Varnish Cache	2.1.2	All	All	All
Application	Varnish Cache Project	Varnish Cache	2.1.3	All	All	All
Application	Varnish Cache Project	Varnish Cache	2.1.4	All	All	All
Application	Varnish Cache Project	Varnish Cache	2.1.5	All	All	All
Application	Varnish Cache Project	Varnish Cache	3.0.0	All	All	All
Application	Varnish Cache Project	Varnish Cache	3.0.0	beta1	All	All
Application	Varnish Cache Project	Varnish Cache	3.0.0	beta2	All	All
Application	Varnish Cache Project	Varnish Cache	3.0.1	All	All	All
Application	Varnish Cache Project	Varnish Cache	3.0.2	All	All	All
Application	Varnish Cache Project	Varnish Cache	3.0.3	All	All	All
Application	Varnish Cache Project	Varnish Cache	All	All	All	All

References

Reference	Source	Link
oss-security - Re: CVE number needed for Varnish DoS, also heads-up	MLIST	www.openwall.com
Security Advisory SA55746 - Debian update for varnish - Secunia	SECUNIA	secunia.com
Security Advisory SA55452 - Varnish GET Requests Handling Denial of Service Vulnerability - Secunia	SECUNIA	secunia.com
openSUSE-SU-2013:1683-1: moderate: update for varnish	SUSE	lists.opensuse.org
#1367 (Varnish crashes if GET consists from whitespaces only) – Varnish	CONFIRM	www.varnish-cache.org
openSUSE-SU-2013:1679-1: moderate: update for varnish	SUSE	lists.opensuse.org
20131030 [CVE-2013-4484] DoS vulnerability in Varnish HTTP cache	BUGTRAQ	archives.neohapsis.com
Debian -- Page not found	DEBIAN	www.debian.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.

There are currently no legacy QID mappings associated with this CVE.

© 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