



CVE-2015-8852

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

Summary

CVE	CVE-2015-8852
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2016-04-25 14:59:00 UTC
Updated	2022-08-02 16:29:00 UTC
Description	Varnish 3.x before 3.0.7, when used in certain stacked installations, allows remote attackers to inject arbitrary HTTP headers.

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	7.0	All	All	All
Operating System	Debian	Debian Linux	7.0	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	3.0.4	All	All	All
Application	Varnish-cache	Varnish	3.0.5	All	All	All
Application	Varnish-cache	Varnish	3.0.6	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	3.0.4	All	All	All
Application	Varnish-cache	Varnish	3.0.5	All	All	All

Application	Varnish-cache	Varnish	3.0.6	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	3.0.4	All	All	All
Application	Varnish-cache	Varnish Cache	3.0.5	All	All	All
Application	Varnish-cache	Varnish Cache	3.0.6	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	3.0.4	All	All	All
Application	Varnish Cache Project	Varnish Cache	3.0.5	All	All	All
Application	Varnish Cache Project	Varnish Cache	3.0.6	All	All	All

References

Reference	Score
oss-security - Re: CVE request: Varnish 3 before 3.0.7 was vulnerable to HTTP Smuggling issues: Double Content Length and bad EOL	Medium
Varnish 3.0.7 released.	Medium
oss-security - CVE request: Varnish 3 before 3.0.7 was vulnerable to HTTP Smuggling issues: Double Content Length and bad EOL	Medium
Do not consider a CR by itself as a valid line terminator · varnish/Varnish-Cache@85e8468 · GitHub	Confidential
Debian -- Security Information -- DSA-3553-1 varnish	Debian
openSUSE-SU-2016:1316-1: moderate: Security update for varnish	SUSE
Varnish: Multiple vulnerabilities (GLSA 201607-10) — Gentoo security	Gentoo
Check for duplicate Content-Length headers in requests · varnish/Varnish-Cache@29870c8 · GitHub	Confidential
CVE Program record	CVE
NVD vulnerability detail	NVD

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](#)