



CVE-2005-0291

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

Summary

CVE	CVE-2005-0291
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2005-01-17 05:00:00 UTC
Updated	2017-07-11 01:32:00 UTC
Description	Cross-site scripting (XSS) vulnerability in the log viewer in NETGEAR FVS318 running firmware 2.4, and possibly other ver:

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Netgear	Fvs318	2.4	All	All	All
Hardware	Netgear	Fvs318	2.4	All	All	All

References

Reference
NetGear FVS318 ProSafe VPN Firewall Switch Multiple Vulnerabilities
securinews.com
13012
[Full-Disclosure] Multiple Vulnerabilities in Netgear FVS318 Router
Secunia - Advisories - Netgear FVS318 Two Vulnerabilities
IBM X-Force Exchange
SecurityTracker.com Archives - NETGEAR FVS318 Lets Remote Users Bypass the URL Filter and Conduct Cross-Site Scripting Attacks Agai
'Multiple Vulnerabilities in Netgear FVS318 Router' - MARC
CVE Program record
NVD vulnerability detail

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](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)