



CVE-2016-3194

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

Summary

CVE	CVE-2016-3194
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2016-08-19 21:59:00 UTC
Updated	2017-08-16 01:29:00 UTC
Description	Cross-site scripting (XSS) vulnerability in the address added page in Fortinet FortiManager 5.x before 5.0.12 and 5.2.x before

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Fortinet	Fortianalyzer Firmware	5.0.0	All	All	All
Operating System	Fortinet	Fortianalyzer Firmware	5.0.10	All	All	All
Operating System	Fortinet	Fortianalyzer Firmware	5.0.11	All	All	All
Operating System	Fortinet	Fortianalyzer Firmware	5.0.12	All	All	All
Operating System	Fortinet	Fortianalyzer Firmware	5.0.2	All	All	All
Operating System	Fortinet	Fortianalyzer Firmware	5.0.3	All	All	All
Operating System	Fortinet	Fortianalyzer Firmware	5.0.4	All	All	All
Operating System	Fortinet	Fortianalyzer Firmware	5.0.5	All	All	All
Operating System	Fortinet	Fortianalyzer Firmware	5.0.6	All	All	All
Operating System	Fortinet	Fortianalyzer Firmware	5.0.7	All	All	All
Operating System	Fortinet	Fortianalyzer Firmware	5.0.8	All	All	All
Operating System	Fortinet	Fortianalyzer Firmware	5.0.9	All	All	All
Operating System	Fortinet	Fortianalyzer Firmware	5.2.0	All	All	All
Operating System	Fortinet	Fortianalyzer Firmware	5.2.1	All	All	All
Operating System	Fortinet	Fortianalyzer Firmware	5.2.2	All	All	All
Operating System	Fortinet	Fortianalyzer Firmware	5.2.3	All	All	All
Operating System	Fortinet	Fortianalyzer Firmware	5.2.4	All	All	All

Operating System	Fortinet	Fortimanager Firmware	5.2.4	All	All	All
Operating System	Fortinet	Fortimanager Firmware	5.2.5	All	All	All
Operating System	Fortinet	Fortimanager Firmware	5.0.0	All	All	All
Operating System	Fortinet	Fortimanager Firmware	5.0.1	All	All	All
Operating System	Fortinet	Fortimanager Firmware	5.0.10	All	All	All
Operating System	Fortinet	Fortimanager Firmware	5.0.11	All	All	All
Operating System	Fortinet	Fortimanager Firmware	5.0.2	All	All	All
Operating System	Fortinet	Fortimanager Firmware	5.0.3	All	All	All
Operating System	Fortinet	Fortimanager Firmware	5.0.4	All	All	All
Operating System	Fortinet	Fortimanager Firmware	5.0.5	All	All	All
Operating System	Fortinet	Fortimanager Firmware	5.0.6	All	All	All
Operating System	Fortinet	Fortimanager Firmware	5.0.7	All	All	All
Operating System	Fortinet	Fortimanager Firmware	5.0.8	All	All	All
Operating System	Fortinet	Fortimanager Firmware	5.0.9	All	All	All
Operating System	Fortinet	Fortimanager Firmware	5.2.0	All	All	All
Operating System	Fortinet	Fortimanager Firmware	5.2.1	All	All	All
Operating System	Fortinet	Fortimanager Firmware	5.2.2	All	All	All
Operating System	Fortinet	Fortimanager Firmware	5.2.3	All	All	All
Operating System	Fortinet	Fortimanager Firmware	5.2.4	All	All	All
Operating System	Fortinet	Fortimanager Firmware	5.2.5	All	All	All

References

Reference

[Fortinet FortiAnalyzer Input Validation Flaw in Image Uploading Lets Remote Authenticated Users Conduct Cross-Site Scripting Attacks - SecWiki](#)

[FortiManager and FortiAnalyzer XSS vulnerability | FortiGuard.com](#)

[FortiManager and FortiAnalyzer CVE-2016-3194 Cross Site Scripting Vulnerability](#)

[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.

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](#)