



CVE-2017-7739

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

Summary

CVE	CVE-2017-7739
State	PUBLIC
Assigner	psirt@fortinet.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-11-13 14:29:00 UTC
Updated	2017-11-29 15:18:00 UTC
Description	A reflected Cross-site Scripting (XSS) vulnerability in web proxy disclaimer response web pages in Fortinet FortiOS 5.6.0, 5

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Fortinet	Fortios	5.2.0	All	All	All
Operating System	Fortinet	Fortios	5.2.1	All	All	All
Operating System	Fortinet	Fortios	5.2.10	All	All	All
Operating System	Fortinet	Fortios	5.2.11	All	All	All
Operating System	Fortinet	Fortios	5.2.2	All	All	All
Operating System	Fortinet	Fortios	5.2.3	All	All	All
Operating System	Fortinet	Fortios	5.2.4	All	All	All
Operating System	Fortinet	Fortios	5.2.5	All	All	All
Operating System	Fortinet	Fortios	5.2.6	All	All	All
Operating System	Fortinet	Fortios	5.2.7	All	All	All
Operating System	Fortinet	Fortios	5.2.8	All	All	All
Operating System	Fortinet	Fortios	5.2.9	All	All	All
Operating System	Fortinet	Fortios	5.4.0	All	All	All
Operating System	Fortinet	Fortios	5.4.1	All	All	All
Operating System	Fortinet	Fortios	5.4.2	All	All	All
Operating System	Fortinet	Fortios	5.4.3	All	All	All
Operating System	Fortinet	Fortios	5.4.4	All	All	All

Operating System	Fortinet	Fortios	5.4.5	All	All	All
Operating System	Fortinet	Fortios	5.6.0	All	All	All
Operating System	Fortinet	Fortios	5.2.0	All	All	All
Operating System	Fortinet	Fortios	5.2.1	All	All	All
Operating System	Fortinet	Fortios	5.2.10	All	All	All
Operating System	Fortinet	Fortios	5.2.11	All	All	All
Operating System	Fortinet	Fortios	5.2.2	All	All	All
Operating System	Fortinet	Fortios	5.2.3	All	All	All
Operating System	Fortinet	Fortios	5.2.4	All	All	All
Operating System	Fortinet	Fortios	5.2.5	All	All	All
Operating System	Fortinet	Fortios	5.2.6	All	All	All
Operating System	Fortinet	Fortios	5.2.7	All	All	All
Operating System	Fortinet	Fortios	5.2.8	All	All	All
Operating System	Fortinet	Fortios	5.2.9	All	All	All
Operating System	Fortinet	Fortios	5.4.0	All	All	All
Operating System	Fortinet	Fortios	5.4.1	All	All	All
Operating System	Fortinet	Fortios	5.4.2	All	All	All
Operating System	Fortinet	Fortios	5.4.3	All	All	All
Operating System	Fortinet	Fortios	5.4.4	All	All	All
Operating System	Fortinet	Fortios	5.4.5	All	All	All
Operating System	Fortinet	Fortios	5.6.0	All	All	All

References

Reference
FortiOS Reflected XSS in Web Proxy Disclaimer Response web page FortiGuard
Fortinet FortiOS Input Validation Flaw in Web Proxy Disclaimer Response Lets Remote Users Conduct Cross-Site Scripting Attacks - Security
Fortinet FortiOS CVE-2017-7739 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.

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