



CVE-2017-7732

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

Summary

CVE	CVE-2017-7732
State	PUBLIC
Assigner	psirt@fortinet.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-10-26 13:29:00 UTC
Updated	2017-11-17 18:18:00 UTC
Description	A reflected Cross-Site Scripting (XSS) vulnerability in Fortinet FortiMail 5.1 and earlier, 5.2.0 through 5.2.9, and 5.3.0 through 5.3.9.

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Fortinet	Fortimail	4.1.0	All	All	All
Application	Fortinet	Fortimail	4.2.0	All	All	All
Application	Fortinet	Fortimail	4.3.0	All	All	All
Application	Fortinet	Fortimail	4.3.8	All	All	All
Application	Fortinet	Fortimail	5.0	All	All	All
Application	Fortinet	Fortimail	5.0.1	All	All	All
Application	Fortinet	Fortimail	5.0.10	All	All	All
Application	Fortinet	Fortimail	5.0.2	All	All	All
Application	Fortinet	Fortimail	5.0.3	All	All	All
Application	Fortinet	Fortimail	5.0.4	All	All	All
Application	Fortinet	Fortimail	5.0.5	All	All	All
Application	Fortinet	Fortimail	5.0.6	All	All	All
Application	Fortinet	Fortimail	5.0.7	All	All	All
Application	Fortinet	Fortimail	5.0.8	All	All	All
Application	Fortinet	Fortimail	5.0.9	All	All	All
Application	Fortinet	Fortimail	5.1	All	All	All
Application	Fortinet	Fortimail	5.2	All	All	All

Application	Fortinet	Fortimail	5.2.1	All	All	All
Application	Fortinet	Fortimail	5.2.2	All	All	All
Application	Fortinet	Fortimail	5.2.3	All	All	All
Application	Fortinet	Fortimail	5.2.4	All	All	All
Application	Fortinet	Fortimail	5.2.5	All	All	All
Application	Fortinet	Fortimail	5.2.6	All	All	All
Application	Fortinet	Fortimail	5.2.7	All	All	All
Application	Fortinet	Fortimail	5.2.8	All	All	All
Application	Fortinet	Fortimail	5.2.9	All	All	All
Application	Fortinet	Fortimail	5.3	All	All	All
Application	Fortinet	Fortimail	5.3.1	All	All	All
Application	Fortinet	Fortimail	5.3.2	All	All	All
Application	Fortinet	Fortimail	5.3.3	All	All	All
Application	Fortinet	Fortimail	5.3.4	All	All	All
Application	Fortinet	Fortimail	5.3.5	All	All	All
Application	Fortinet	Fortimail	5.3.6	All	All	All
Application	Fortinet	Fortimail	5.3.7	All	All	All
Application	Fortinet	Fortimail	5.3.8	All	All	All
Application	Fortinet	Fortimail	5.3.9	All	All	All
Application	Fortinet	Fortimail	4.1.0	All	All	All
Application	Fortinet	Fortimail	4.2.0	All	All	All
Application	Fortinet	Fortimail	4.3.0	All	All	All
Application	Fortinet	Fortimail	4.3.8	All	All	All
Application	Fortinet	Fortimail	5.0	All	All	All
Application	Fortinet	Fortimail	5.0.1	All	All	All
Application	Fortinet	Fortimail	5.0.10	All	All	All
Application	Fortinet	Fortimail	5.0.2	All	All	All
Application	Fortinet	Fortimail	5.0.3	All	All	All
Application	Fortinet	Fortimail	5.0.4	All	All	All
Application	Fortinet	Fortimail	5.0.5	All	All	All
Application	Fortinet	Fortimail	5.0.6	All	All	All
Application	Fortinet	Fortimail	5.0.7	All	All	All
Application	Fortinet	Fortimail	5.0.8	All	All	All
Application	Fortinet	Fortimail	5.0.9	All	All	All
Application	Fortinet	Fortimail	5.1	All	All	All

Application	Fortinet	Fortimail	5.2	All	All	All
Application	Fortinet	Fortimail	5.2.1	All	All	All
Application	Fortinet	Fortimail	5.2.2	All	All	All
Application	Fortinet	Fortimail	5.2.3	All	All	All
Application	Fortinet	Fortimail	5.2.4	All	All	All
Application	Fortinet	Fortimail	5.2.5	All	All	All
Application	Fortinet	Fortimail	5.2.6	All	All	All
Application	Fortinet	Fortimail	5.2.7	All	All	All
Application	Fortinet	Fortimail	5.2.8	All	All	All
Application	Fortinet	Fortimail	5.2.9	All	All	All
Application	Fortinet	Fortimail	5.3	All	All	All
Application	Fortinet	Fortimail	5.3.1	All	All	All
Application	Fortinet	Fortimail	5.3.2	All	All	All
Application	Fortinet	Fortimail	5.3.3	All	All	All
Application	Fortinet	Fortimail	5.3.4	All	All	All
Application	Fortinet	Fortimail	5.3.5	All	All	All
Application	Fortinet	Fortimail	5.3.6	All	All	All
Application	Fortinet	Fortimail	5.3.7	All	All	All
Application	Fortinet	Fortimail	5.3.8	All	All	All
Application	Fortinet	Fortimail	5.3.9	All	All	All

References

Reference

Fortinet FortiMail CVE-2017-7732 Cross Site Scripting Vulnerability

Fortinet FortiMail Input Validation Flaw in Customized Webmail Login Page Lets Remote Users Conduct Cross-Site Scripting Attacks - SecurityWeek

FortiMail reflected XSS vulnerability under customized webmail login page | FortiGuard

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](#).

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report