CVE-2015-1880

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2015-1880
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-05-12 19:59:00 UTC
Updated	2017-01-03 18:39:00 UTC
Description	Cross-site scripting (XSS) vulnerability in the sslvpn login page in Fortinet FortiOS 5.2.x before 5.2.3 allows remote attacker

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	5.2.2	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	5.2.2	All	All	All

References

Reference
Fortinet FortiMail Input Validation Flaws in SSLVPN Login Page, User Group Menu, and VPN Template Menu Permit Cross-Site Scripting Atta
Fortinet FortiOS CVE-2015-1880 Cross Site Scripting Vulnerability
Fortinet FortiManager Input Validation Flaws in SSLVPN Login Page, User Group Menu, VPN Template Menu, and Advanced Dataset Report
Fortinet FortiGate Input Validation Flaws in SSLVPN Login Page, User Group Menu, and VPN Template Menu Permit Cross-Site Scripting Att
FortiGuard.com | Multiple products cross-site scripting vulnerabilities
Fortinet FortiADC Input Validation Flaws in SSLVPN Login Page, User Group Menu, VPN Template Menu, and Theme Login Page Permit Cro
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.

Free CVE JSON API cve.report/api

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