CVE-2013-7181

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

Summary

CVE	CVE-2013-7181
State	PUBLIC
Assigner	cert@cert.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-02-04 05:39:00 UTC
Updated	2015-07-27 16:12:00 UTC
Description	Cross-site scripting (XSS) vulnerability in user/ldap_user/add in Fortinet FortiOS 5.0.3 allows remote attackers to inject arbi

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Fortinet	Fortiweb	5.0.3	All	All	All
Application	Fortinet	Fortiweb	5.0.3	All	All	All

References

Reference	Source	Link
20140203 XSS Reflected vulnerabilities in OS of FortiWeb v 5.0.3 (CVE-2013-7181)	FULLDISC	archive
Fortinet Fortiweb 'filter' Parameter Cross Site Scripting Vulnerability	BID	www.s
FortiGuard.com | FortiWeb Cross-Site Scripting Vulnerability	CONFIRM	www.f
Security Advisory SA56732 - Fortinet FortiWeb "filter" Cross-Site Scripting Vulnerability - Secunia	SECUNIA	secuni
102820	OSVDB	osvdb.
Fortinet FortiWeb Input Validation Flaw in '/user/ldap_user/add' Permits Cross-Site Scripting Attacks - SecurityTracker	SECTRACK	www.s
Vulnerability Note VU#593118 - Fortinet Fortiweb 5.0.3 contains a reflected cross-site scripting vulnerability	CERT-VN	www.k
CVE Program record	CVE.ORG	www.c
NVD vulnerability detail	NVD	nvd.ni

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**