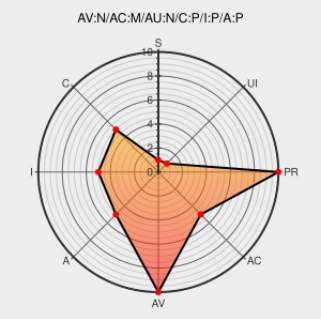
CVE-2014-3115

Published on: 05/08/2014 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:46 PM UTC

CVE-2014-3115

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Fortiweb from Fortinet contain the following vulnerability:

Multiple cross-site request forgery (CSRF) vulnerabilities in the web administration console in Fortinet FortiWeb before 5.2.0 allow remote attackers to hijack the authentication of administrators via system/config/adminadd and other unspecified vectors.

CVE-2014-3115 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 6.8 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
FortiGuard.com | FortiWeb Cross-Site Request Forgery Vulnerability	Vendor Advisory, www.fortiguard.com, text/html	CONFIRM www.fortiguard.com/advisory/FG-IR-14-013/
Full Disclosure: Fortinet Fortiweb 5.1 contains a cross-site request forgery vulnerability (CVE-2014-3115)	seclists.org, text/html	FULLDISC 20140507 Fortinet Fortiweb 5.1 contains a cross-site request forgery vulnerability (CVE-2014-3115)
Fortinet FortiWeb Input Validation Flaw Permits Cross-Site Request Forgery Attacks - SecurityTracker	www.securitytracker.com, text/html	SECTRACK 1030200
Vulnerability Note VU#902790 - Fortinet Fortiweb 5.1 contains a cross-site request forgery vulnerability	US Government Resource, www.kb.cert.org, text/html	CERT-VN VU#902790

are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Fortinet	Fortiweb	5.1.0	All	All	All
Application	Fortinet	Fortiweb	5.1.1	All	All	All
Application	Fortinet	Fortiweb	5.1.2	All	All	All
Application	Fortinet	Fortiweb	5.1.3	All	All	All
Application	Fortinet	Fortiweb	5.1.0	All	All	All
Application	Fortinet	Fortiweb	5.1.1	All	All	All
Application	Fortinet	Fortiweb	5.1.2	All	All	All
Application	Fortinet	Fortiweb	5.1.3	All	All	All
Application	Fortinet	Fortiweb	All	All	All	All

cpe:2.3:a:fortinet:fortiweb:5.1.0:*:*:*:*:*:*:*:

cpe:2.3:a:fortinet:fortiweb:5.1.1:*:*:*:*:*:*:*:

cpe:2.3:a:fortinet:fortiweb:5.1.2:*:*:*:*:*:*:*:

cpe:2.3:a:fortinet:fortiweb:5.1.3:*:*:*:*:*:*:*:

cpe:2.3:a:fortinet:fortiweb:5.1.0:*:*:*:*:*:*:*:

cpe:2.3:a:fortinet:fortiweb:5.1.1:*:*:*:*:*:*:*:

cpe:2.3:a:fortinet:fortiweb:5.1.2:*:*:*:*:*:*:*:

cpe:2.3:a:fortinet:fortiweb:5.1.3:*:*:*:*:*:*:*:

cpe:2.3:a:fortinet:fortiweb:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

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