



CVE-2014-8619

Published on: 05/12/2015 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:51 PM UTC

CVE-2014-8619

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



Certain versions of **Fortiweb** from **Fortinet** contain the following vulnerability:

Cross-site scripting (XSS) vulnerability in the autolearn configuration page in Fortinet FortiWeb 5.1.2 through 5.3.4 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.

CVE-2014-8619 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: **4.3 - MEDIUM**

Access
Vector

NETWORK

Access
Complexity

MEDIUM

Authentication

NONE

Confidentiality
Impact

NONE

Integrity
Impact

PARTIAL

Availability
Impact

NONE

CVE References

Description

Tags

Link

Fortinet FortiWeb Input Validation Flaw in Autolearn Configuration Page Permits Cross-Site Scripting Attacks - SecurityTracker

www.securitytracker.com
text/html

[SECTRACK 1032307](https://sectrack.com/sectrack/1032307)

FortiGuard.com | Multiple products cross-site scripting vulnerabilities

Vendor Advisory
www.fortiguard.com
text/html

CONFIRM
www.fortiguard.com/advisory/FG-IR-15-005/

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that 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	5.1.2	All	All	All
Application	Fortinet	Fortiweb	5.1.3	All	All	All
Application	Fortinet	Fortiweb	5.1.4	All	All	All
Application	Fortinet	Fortiweb	5.2.0	All	All	All
Application	Fortinet	Fortiweb	5.2.1	All	All	All
Application	Fortinet	Fortiweb	5.2.2	All	All	All
Application	Fortinet	Fortiweb	5.2.3	All	All	All
Application	Fortinet	Fortiweb	5.2.4	All	All	All
Application	Fortinet	Fortiweb	5.3.0	All	All	All
Application	Fortinet	Fortiweb	5.3.1	All	All	All
Application	Fortinet	Fortiweb	5.3.2	All	All	All
Application	Fortinet	Fortiweb	5.3.3	All	All	All
Application	Fortinet	Fortiweb	5.3.4	All	All	All
Application	Fortinet	Fortiweb	5.1.2	All	All	All
Application	Fortinet	Fortiweb	5.1.3	All	All	All
Application	Fortinet	Fortiweb	5.1.4	All	All	All
Application	Fortinet	Fortiweb	5.2.0	All	All	All
Application	Fortinet	Fortiweb	5.2.1	All	All	All
Application	Fortinet	Fortiweb	5.2.2	All	All	All
Application	Fortinet	Fortiweb	5.2.3	All	All	All
Application	Fortinet	Fortiweb	5.2.4	All	All	All
Application	Fortinet	Fortiweb	5.3.0	All	All	All
Application	Fortinet	Fortiweb	5.3.1	All	All	All
Application	Fortinet	Fortiweb	5.3.2	All	All	All
Application	Fortinet	Fortiweb	5.3.3	All	All	All
Application	Fortinet	Fortiweb	5.3.4	All	All	All
cpe:2.3:a:fortinet:fortiweb:5.1.2:*****:						
cpe:2.3:a:fortinet:fortiweb:5.1.3:*****:						
cpe:2.3:a:fortinet:fortiweb:5.1.4:*****:						
cpe:2.3:a:fortinet:fortiweb:5.2.0:*****:						
cpe:2.3:a:fortinet:fortiweb:5.2.1:*****:						
cpe:2.3:a:fortinet:fortiweb:5.2.2:*****:						
cpe:2.3:a:fortinet:fortiweb:5.2.3:*****:						
cpe:2.3:a:fortinet:fortiweb:5.2.4:*****:						
cpe:2.3:a:fortinet:fortiweb:5.3.0:*****:						
cpe:2.3:a:fortinet:fortiweb:5.3.1:*****:						
cpe:2.3:a:fortinet:fortiweb:5.3.2:*****:						
cpe:2.3:a:fortinet:fortiweb:5.3.3:*****:						
cpe:2.3:a:fortinet:fortiweb:5.3.4:*****:						

No vendor comments have been submitted for this CVE

Next ID→

