



CVE-2015-2323

Published on: 08/11/2015 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:21 PM UTC

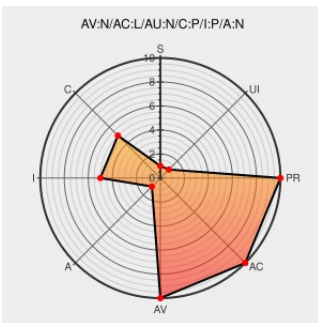
CVE-2015-2323

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



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

FortiOS 5.0.x before 5.0.12 and 5.2.x before 5.2.4 supports anonymous, export, RC4, and possibly other weak ciphers when using TLS to connect to FortiGuard servers, which allows man-in-the-middle attackers to spoof TLS content by modifying packets.

CVE-2015-2323 has been assigned by [M cve@mitre.org](mailto:cve@mitre.org) to track the vulnerability

CVSS2 Score: **6.4 - MEDIUM**

Access
Vector

NETWORK

Access
Complexity

LOW

Authentication

NONE

Confidentiality
Impact

PARTIAL

Integrity
Impact

PARTIAL

Availability
Impact

NONE

CVE References

Description

Tags

Link

FortiGuard

fortiguard.com

[text/html](#)

[Inactive Link](#) [Not Archived](#)

[CONFIRM fortiguard.com/advisory/2015-07-24-weak-ciphers-suites-are-presented-towards-fortiguard-servers](http://fortiguard.com/advisory/2015-07-24-weak-ciphers-suites-are-presented-towards-fortiguard-servers)

Fortinet FortiGate/FortiOS Weak Encryption Lets Remote Users Decrypt and Modify Data - SecurityTracker

www.securitytracker.com

[text/html](#)

[SECTRAK 1033092](https://www.sectrack.com/1033092)

FortiOS supports weak ciphers suites when connecting to Fortiguard servers | FortiGuard

[Vendor Advisory](#)

www.fortiguard.com

[text/html](#)

[CONFIRM www.fortiguard.com/advisory/FG-IR-15-021/](http://fortiguard.com/advisory/FG-IR-15-021/)

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
Operating System	Fortinet	Fortios	5.0.0	All	All	All
Operating System	Fortinet	Fortios	5.0.1	All	All	All
Operating System	Fortinet	Fortios	5.0.10	All	All	All
Operating System	Fortinet	Fortios	5.0.11	All	All	All
Operating System	Fortinet	Fortios	5.0.2	All	All	All
Operating System	Fortinet	Fortios	5.0.3	All	All	All
Operating System	Fortinet	Fortios	5.0.4	All	All	All
Operating System	Fortinet	Fortios	5.0.5	All	All	All
Operating System	Fortinet	Fortios	5.0.6	All	All	All
Operating System	Fortinet	Fortios	5.0.7	All	All	All
Operating System	Fortinet	Fortios	5.0.8	All	All	All
Operating System	Fortinet	Fortios	5.0.9	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
Operating System	Fortinet	Fortios	5.2.3	All	All	All
Operating System	Fortinet	Fortios	5.0.0	All	All	All
Operating System	Fortinet	Fortios	5.0.1	All	All	All
Operating System	Fortinet	Fortios	5.0.10	All	All	All
Operating System	Fortinet	Fortios	5.0.11	All	All	All

Operating System	Fortinet	Fortios	5.0.2	All	All	All
Operating System	Fortinet	Fortios	5.0.3	All	All	All
Operating System	Fortinet	Fortios	5.0.4	All	All	All
Operating System	Fortinet	Fortios	5.0.5	All	All	All
Operating System	Fortinet	Fortios	5.0.6	All	All	All
Operating System	Fortinet	Fortios	5.0.7	All	All	All
Operating System	Fortinet	Fortios	5.0.8	All	All	All
Operating System	Fortinet	Fortios	5.0.9	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
Operating System	Fortinet	Fortios	5.2.3	All	All	All
cpe:2.3:o:fortinet:fortios:5.0.0:*****:						
cpe:2.3:o:fortinet:fortios:5.0.1:*****:						
cpe:2.3:o:fortinet:fortios:5.0.10:*****:						
cpe:2.3:o:fortinet:fortios:5.0.11:*****:						
cpe:2.3:o:fortinet:fortios:5.0.2:*****:						
cpe:2.3:o:fortinet:fortios:5.0.3:*****:						
cpe:2.3:o:fortinet:fortios:5.0.4:*****:						
cpe:2.3:o:fortinet:fortios:5.0.5:*****:						
cpe:2.3:o:fortinet:fortios:5.0.6:*****:						
cpe:2.3:o:fortinet:fortios:5.0.7:*****:						
cpe:2.3:o:fortinet:fortios:5.0.8:*****:						
cpe:2.3:o:fortinet:fortios:5.0.9:*****:						
cpe:2.3:o:fortinet:fortios:5.2.0:*****:						
cpe:2.3:o:fortinet:fortios:5.2.1:*****:						

cpe:2.3:o:fortinet:fortios:5.2.1:*****:
cpe:2.3:o:fortinet:fortios:5.2.2:*****:
cpe:2.3:o:fortinet:fortios:5.2.3:*****:
cpe:2.3:o:fortinet:fortios:5.0.0:*****:
cpe:2.3:o:fortinet:fortios:5.0.1:*****:
cpe:2.3:o:fortinet:fortios:5.0.10:*****:
cpe:2.3:o:fortinet:fortios:5.0.11:*****:
cpe:2.3:o:fortinet:fortios:5.0.2:*****:
cpe:2.3:o:fortinet:fortios:5.0.3:*****:
cpe:2.3:o:fortinet:fortios:5.0.4:*****:
cpe:2.3:o:fortinet:fortios:5.0.5:*****:
cpe:2.3:o:fortinet:fortios:5.0.6:*****:
cpe:2.3:o:fortinet:fortios:5.0.7:*****:
cpe:2.3:o:fortinet:fortios:5.0.8:*****:
cpe:2.3:o:fortinet:fortios:5.0.9:*****:
cpe:2.3:o:fortinet:fortios:5.2.0:*****:
cpe:2.3:o:fortinet:fortios:5.2.1:*****:
cpe:2.3:o:fortinet:fortios:5.2.2:*****:
cpe:2.3:o:fortinet:fortios:5.2.3:*****:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)