



# CVE-2015-3620

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

## Summary

<b>CVE</b>	CVE-2015-3620
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2015-05-12 19:59:00 UTC
<b>Updated</b>	2018-10-09 19:56:00 UTC
<b>Description</b>	Cross-site scripting (XSS) vulnerability in the advanced dataset reports page in Fortinet FortiAnalyzer 5.0.0 through 5.0.10

## Risk And Classification

**Problem Types:** CWE-79

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Fortinet	Fortianalyzer Firmware	5.0.0	All	All	All
Operating System	Fortinet	Fortianalyzer Firmware	5.0.1	All	All	All
Operating System	Fortinet	Fortianalyzer Firmware	5.0.10	All	All	All
Operating System	Fortinet	Fortianalyzer Firmware	5.2.0	All	All	All
Operating System	Fortinet	Fortianalyzer Firmware	5.2.1	All	All	All
Operating System	Fortinet	Fortianalyzer Firmware	5.0.0	All	All	All
Operating System	Fortinet	Fortianalyzer Firmware	5.0.1	All	All	All
Operating System	Fortinet	Fortianalyzer Firmware	5.0.10	All	All	All
Operating System	Fortinet	Fortianalyzer Firmware	5.2.0	All	All	All
Operating System	Fortinet	Fortianalyzer Firmware	5.2.1	All	All	All
Operating System	Fortinet	Fortimanager Firmware	5.0.10	All	All	All
Operating System	Fortinet	Fortimanager Firmware	5.0.3	All	All	All
Operating System	Fortinet	Fortimanager Firmware	5.0.4	All	All	All
Operating System	Fortinet	Fortimanager Firmware	5.0.5	All	All	All
Operating System	Fortinet	Fortimanager Firmware	5.0.6	All	All	All
Operating System	Fortinet	Fortimanager Firmware	5.0.7	All	All	All
Operating System	Fortinet	Fortimanager Firmware	5.0.8	All	All	All

Operating System	<a href="#">Fortinet</a>	<a href="#">Fortimanager Firmware</a>	5.0.9	All	All	All
Operating System	<a href="#">Fortinet</a>	<a href="#">Fortimanager Firmware</a>	5.2.0	All	All	All
Operating System	<a href="#">Fortinet</a>	<a href="#">Fortimanager Firmware</a>	5.2.1	All	All	All
Operating System	<a href="#">Fortinet</a>	<a href="#">Fortimanager Firmware</a>	5.0.10	All	All	All
Operating System	<a href="#">Fortinet</a>	<a href="#">Fortimanager Firmware</a>	5.0.3	All	All	All
Operating System	<a href="#">Fortinet</a>	<a href="#">Fortimanager Firmware</a>	5.0.4	All	All	All
Operating System	<a href="#">Fortinet</a>	<a href="#">Fortimanager Firmware</a>	5.0.5	All	All	All
Operating System	<a href="#">Fortinet</a>	<a href="#">Fortimanager Firmware</a>	5.0.6	All	All	All
Operating System	<a href="#">Fortinet</a>	<a href="#">Fortimanager Firmware</a>	5.0.7	All	All	All
Operating System	<a href="#">Fortinet</a>	<a href="#">Fortimanager Firmware</a>	5.0.8	All	All	All
Operating System	<a href="#">Fortinet</a>	<a href="#">Fortimanager Firmware</a>	5.0.9	All	All	All
Operating System	<a href="#">Fortinet</a>	<a href="#">Fortimanager Firmware</a>	5.2.0	All	All	All
Operating System	<a href="#">Fortinet</a>	<a href="#">Fortimanager Firmware</a>	5.2.1	All	All	All

## References

### Reference

[Fortinet FortiAnalyzer / FortiManager Cross Site Scripting ≈ Packet Storm](#)

[Full Disclosure: Fortinet FortiAnalyzer & FortiManager - Client Side Cross Site Scripting Vulnerability](#)

[FortiAnalyzer and FortiManager CVE-2015-3620 Cross Site Scripting Vulnerability](#)

[SecurityFocus](#)

[Fortinet FortiManager Input Validation Flaws in SSLVPN Login Page, User Group Menu, VPN Template Menu, and Advanced Dataset Report](#)

[FortiGuard.com | Multiple products cross-site scripting vulnerabilities](#)

[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.

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

**CVE.report and Source URL Uptime Status** [status.cve.report](#)