



CVE-2018-1354

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

Summary

CVE	CVE-2018-1354
State	PUBLIC
Assigner	psirt@fortinet.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-06-27 20:29:00 UTC
Updated	2019-10-03 00:03:00 UTC
Description	An improper access control vulnerability in Fortinet FortiManager 6.0.0, 5.6.5 and below versions, FortiAnalyzer 6.0.0, 5.6.5

Risk And Classification

Problem Types: CWE-732

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Fortinet	Fortianalyzer	All	All	All	All
Application	Fortinet	Fortimanager	All	All	All	All

References

Reference	Source	Link
FortiAnalyzer and FortiManager admin user avatar setting improper access control FortiGuard	CONFIRM	fortigu...
Fortinet FortiManager Flaw Lets Remote Authenticated Users Modify Avatars on the Target System - SecurityTracker	SECTRACK	www.s...
Fortinet FortiAnalyzer and FortiManager CVE-2018-1354 Access Bypass Vulnerability	BID	www.s...
Fortinet FortiAnalyzer Flaw Lets Remote Authenticated Users Modify Avatars on the Target System - SecurityTracker	SECTRACK	www.s...
CVE Program record	CVE.ORG	www.c...
NVD vulnerability detail	NVD	nvd.nis...

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](#).

Free CVE JSON API [cve.report/api](#)

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