



CVE-2023-44249

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

Summary

CVE	CVE-2023-44249
State	PUBLIC
Assigner	psirt@fortinet.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-10-10 17:15:00 UTC
Updated	2023-11-07 04:21:00 UTC
Description	An authorization bypass through user-controlled key [CWE-639] vulnerability in Fortinet FortiManager version 7.4.0 and bef

Risk And Classification

Problem Types: CWE-639

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Fortinet	Fortianalyzer	7.4.0	All	All	All
Application	Fortinet	Fortianalyzer	All	All	All	All
Application	Fortinet	Fortianalyzer	All	All	All	All
Application	Fortinet	Fortianalyzer	All	All	All	All
Application	Fortinet	Fortianalyzer	All	All	All	All
Application	Fortinet	Fortimanager	7.4.0	All	All	All
Application	Fortinet	Fortimanager	All	All	All	All
Application	Fortinet	Fortimanager	All	All	All	All
Application	Fortinet	Fortimanager	All	All	All	All
Application	Fortinet	Fortimanager	All	All	All	All

References

Reference

- Fortinet FortiManager - Asynchronous tasks that use `taskid` in the FortiManager are vulnerable to IDOR vulnerability (CVE-2023-44249) · Ad
- FortiGuard
- CVE Program record
- NVD vulnerability detail

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[379129](#) Fortinet FortiAnalyzer and FortiManager Multiple Vulnerabilities (FG-IR-23-201) (FG-IR-23-187)

© [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](#)