



# CVE-2023-41841

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

## Summary

<b>CVE</b>	CVE-2023-41841
<b>State</b>	PUBLIC
<b>Assigner</b>	psirt@fortinet.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2023-10-10 17:15:00 UTC
<b>Updated</b>	2023-11-07 04:21:00 UTC
<b>Description</b>	An improper authorization vulnerability in Fortinet FortiOS 7.0.0 - 7.0.11 and 7.2.0 - 7.2.4 allows an attacker belonging to th

## Risk And Classification

**Problem Types:** NVD-CWE-Other

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Fortinet	Fortios	All	All	All	All
Operating System	Fortinet	Fortios	All	All	All	All

## References

Reference	Source	Link	Tags
PSIRT Advisories   FortiGuard	MISC	<a href="https://fortiguard.com">fortiguard.com</a>	
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	canonical, analysis

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

44102 FortiOS Privilege Escalation Vulnerability (FG-IR-23-318)

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](https://cve.report/api)

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)