



# CVE-2021-32587

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

## Summary

<b>CVE</b>	CVE-2021-32587
<b>State</b>	PUBLIC
<b>Assigner</b>	psirt@fortinet.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2021-08-06 11:15:00 UTC
<b>Updated</b>	2022-06-28 14:11:00 UTC
<b>Description</b>	An improper access control vulnerability in FortiManager and FortiAnalyzer GUI interface 7.0.0, 6.4.5 and below, 6.2.8 and

## Risk And Classification

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

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Fortinet</a>	<a href="#">Fortianalyzer</a>	All	All	All	All
Application	<a href="#">Fortinet</a>	<a href="#">Fortimanager</a>	All	All	All	All

## References

Reference	Source	Link	Tags
FortiManager & FortiAnalyzer - Improper access control on the administrators account list   FortiGuard	CONFIRM	<a href="#">fortiguard.com</a>	
CVE Program record	CVE.ORG	<a href="#">www.cve.org</a>	canoni
NVD vulnerability detail	NVD	<a href="#">nvd.nist.gov</a>	canoni

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

[376128](#) FortiGate FortiManager and FortiAnalyzer Imporper Access Control Vulnerability (CWE-284)

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](https://status.cve.report)**