



# CVE-2025-68649

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

## Summary

<b>CVE</b>	CVE-2025-68649
<b>State</b>	PUBLISHED
<b>Assigner</b>	fortinet
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-04-14 16:16:34 UTC
<b>Updated</b>	2026-04-22 19:11:36 UTC
<b>Description</b>	An improper limitation of a pathname to a restricted directory ('path traversal') vulnerability in Fortinet FortiAnalyzer 7.6.0 th

## Risk And Classification

**Primary CVSS:** v3.1 6.5 MEDIUM from nvd@nist.gov

**CVSS:** 3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:H/A:H

**EPSS:** 0.000500000 probability, percentile 0.153940000 (date 2026-04-21)

**Problem Types:** CWE-22 | CWE-22 Escalation of privilege

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Primary	6.5	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:H/A:H
3.1	psirt@fortinet.com	Secondary	6	MEDIUM	CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:N/I:H/A:H
3.1	CNA	CVSS	5.4	MEDIUM	CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:N/I:H/A:H/E:P/RL:O/RC:C

## CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

High

User Interaction

None

Scope

Unchanged

Confidentiality

None

Integrity

High

Availability

High

CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:H/A:H

### NVD Known Affected Configurations (CPE 2.3)

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

### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Fortinet	FortiManager Cloud	affected 7.6.2 7.6.4 semver	Not specified
CNA	Fortinet	FortiManager Cloud	affected 7.4.1 7.4.7 semver	Not specified
CNA	Fortinet	FortiManager Cloud	affected 7.2.1 7.2.12 semver	Not specified
CNA	Fortinet	FortiManager Cloud	affected 7.0.1 7.0.16 semver	Not specified
CNA	Fortinet	FortiManager	affected 7.6.0 7.6.4 semver	Not specified
CNA	Fortinet	FortiManager	affected 7.4.0 7.4.7 semver	Not specified
CNA	Fortinet	FortiManager	affected 7.2.0 7.2.12 semver	Not specified
CNA	Fortinet	FortiManager	affected 7.0.0 7.0.16 semver	Not specified
CNA	Fortinet	FortiAnalyzer	affected 7.6.0 7.6.4 semver	Not specified
CNA	Fortinet	FortiAnalyzer	affected 7.4.0 7.4.7 semver	Not specified
CNA	Fortinet	FortiAnalyzer	affected 7.2.0 7.2.12 semver	Not specified
CNA	Fortinet	FortiAnalyzer	affected 7.0.0 7.0.16 semver	Not specified
CNA	Fortinet	FortiAnalyzer Cloud	affected 7.6.2	Not specified
CNA	Fortinet	FortiAnalyzer Cloud	affected 7.4.1 7.4.7 semver	Not specified
CNA	Fortinet	FortiAnalyzer Cloud	affected 7.2.1 7.2.12 semver	Not specified
CNA	Fortinet	FortiAnalyzer Cloud	affected 7.0.1 7.0.16 semver	Not specified

### References

Reference	Source	Link	Tags
fortiguard.fortinet.com/psirt/FG-IR-26-120	psirt@fortinet.com	<a href="https://fortiguard.fortinet.com">fortiguard.fortinet.com</a>	Vendor Advisory
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.

## Additional Advisory Data

### Solutions

**CNA:** Upgrade to FortiManager Cloud version 7.6.5 or above Upgrade to FortiManager Cloud version 7.4.8 or above Upgrade to FortiManager version 7.6.5 or above Upgrade to FortiManager version 7.4.8 or above Upgrade to FortiAnalyzer version 7.6.5 or above Upgrade to FortiAnalyzer version 7.4.8 or above Upgrade to FortiAnalyzer Cloud version 7.6.5 or above Upgrade to FortiAnalyzer Cloud version 7.4.8 or above

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](#)