



# CVE-2026-24858

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2026-24858
<b>State</b>	PUBLISHED
<b>Assigner</b>	fortinet
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-01-27 20:16:24 UTC
<b>Updated</b>	2026-05-12 18:47:28 UTC
<b>Description</b>	An Authentication Bypass Using an Alternate Path or Channel vulnerability [CWE-288] vulnerability in Fortinet FortiAnalyzer

## Risk And Classification

**Primary CVSS:** v3.1 9.8 CRITICAL from psirt@fortinet.com

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

**EPSS:** 0.062070000 probability, percentile 0.909570000 (date 2026-05-12)

**CISA KEV:** Listed on 2026-01-27; due 2026-01-30; ransomware use Unknown

**Problem Types:** CWE-288 | CWE-288 Improper access control

Version	Source	Type	Score	Severity	Vector
3.1	psirt@fortinet.com	Secondary	9.8	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
3.1	CNA	CVSS	9.4	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:H/RL:O/RC:C

## CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

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

### CISA Known Exploited Vulnerability

<b>Vendor</b>	Fortinet
<b>Product</b>	Multiple Products
<b>Name</b>	Fortinet Multiple Products Authentication Bypass Using an Alternate Path or Channel Vulnerability
<b>Required Action</b>	Apply mitigations per vendor instructions, follow applicable BOD 22-01 guidance for cloud services, or discontinue use of the product if mitigations are unavailable.
<b>Notes</b>	Please adhere to Fortinet's guidelines to assess exposure and mitigate risks. Check for signs of potential compromise on all internet accessible Fortinet products affected by this vulnerability. Apply any final mitigations provided by the vendor as soon as they become available. For more information please see: <a href="https://fortiguard.fortinet.com/psirt/FG-IR-26-060">https://fortiguard.fortinet.com/psirt/FG-IR-26-060</a> ; <a href="https://www.fortinet.com/blog/psirt-blogs/analysis-of-ssso-abuse-on-fortios">https://www.fortinet.com/blog/psirt-blogs/analysis-of-ssso-abuse-on-fortios</a> ; <a href="https://nvd.nist.gov/vuln/detail/CVE-2026-24858">https://nvd.nist.gov/vuln/detail/CVE-2026-24858</a>

### NVD Known Affected Configurations (CPE 2.3)

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

### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Fortinet	FortiOS	affected 7.6.0 7.6.5 semver	Not specified
CNA	Fortinet	FortiOS	affected 7.4.0 7.4.10 semver	Not specified
CNA	Fortinet	FortiOS	affected 7.2.0 7.2.12 semver	Not specified
CNA	Fortinet	FortiOS	affected 7.0.0 7.0.18 semver	Not specified
CNA	Fortinet	FortiManager	affected 7.6.0 7.6.5 semver	Not specified
CNA	Fortinet	FortiManager	affected 7.4.0 7.4.9 semver	Not specified
CNA	Fortinet	FortiManager	affected 7.2.0 7.2.11 semver	Not specified
CNA	Fortinet	FortiManager	affected 7.0.0 7.0.15 semver	Not specified
CNA	Fortinet	FortiAnalyzer	affected 7.6.0 7.6.5 semver	Not specified
CNA	Fortinet	FortiAnalyzer	affected 7.4.0 7.4.9 semver	Not specified
CNA	Fortinet	FortiAnalyzer	affected 7.2.0 7.2.11 semver	Not specified
CNA	Fortinet	FortiAnalyzer	affected 7.0.0 7.0.15 semver	Not specified
CNA	Fortinet	FortiProxv	affected 7.6.0 7.6.4 semver	Not specified

CNA	Fortinet	FortiProxy	affected 7.4.0 7.4.12 semver	Not specified
CNA	Fortinet	FortiProxy	affected 7.2.0 7.2.15 semver	Not specified
CNA	Fortinet	FortiProxy	affected 7.0.0 7.0.22 semver	Not specified
CNA	Fortinet	FortiWeb	affected 8.0.0 8.0.3 semver	Not specified
CNA	Fortinet	FortiWeb	affected 7.6.0 7.6.6 semver	Not specified
CNA	Fortinet	FortiWeb	affected 7.4.0 7.4.11 semver	Not specified
ADP	Siemens	RUGGEDCOM APE1808	affected * custom	Not specified

## References

Reference	Source	Link	Tags
fortiguard.fortinet.com/psirt/FG-IR-26-060	psirt@fortinet.com	<a href="https://fortiguard.fortinet.com">fortiguard.fortinet.com</a>	Vendor
www.cisa.gov/known-exploited-vulnerabilities-catalog	134c704f-9b21-4f2e-91b3-4a467353bcc0	<a href="https://www.cisa.gov">www.cisa.gov</a>	US
cert-portal.siemens.com/productcert/html/ssa-975644.html	0b142b55-0307-4c5a-b3c9-f314f3fb7c5e	<a href="https://cert-portal.siemens.com">cert-portal.siemens.com</a>	Third Party
www.fortinet.com/blog/psirt-blogs/analysis-of-ss0-abuse-on-fortios	134c704f-9b21-4f2e-91b3-4a467353bcc0	<a href="https://www.fortinet.com">www.fortinet.com</a>	Microsoft
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
CISA Known Exploited Vulnerabilities catalog	CISA	<a href="https://www.cisa.gov">www.cisa.gov</a>	Key

No vendor comments have been submitted for this CVE.

## Additional Advisory Data

### Solutions

**CNA:** Upgrade to upcoming FortiOS version 8.0.0 or above Upgrade to FortiOS version 7.6.6 or above Upgrade to FortiOS version 7.4.11 or above Upgrade to FortiOS version 7.2.13 or above Upgrade to FortiOS version 7.0.19 or above Upgrade to upcoming FortiManager version 8.0.0 or above Upgrade to FortiManager version 7.6.6 or above Upgrade to FortiManager version 7.4.10 or above Upgrade to FortiManager version 7.2.12 or above Upgrade to FortiManager version 7.0.16 or above Upgrade to FortiAnalyzer version 7.6.6 or above Upgrade to FortiAnalyzer version 7.4.10 or above Upgrade to FortiAnalyzer version 7.2.12 or above Upgrade to FortiAnalyzer version 7.0.16 or above Upgrade to FortiProxy version 7.6.5 or above Upgrade to FortiProxy version 7.4.13 or above Upgrade to FortiProxy version 7.2.16 or above Upgrade to FortiProxy version 7.0.23 or above Upgrade to FortiWeb version 8.0.4 or above Upgrade to FortiWeb version 7.6.7 or above Upgrade to FortiWeb version 7.4.12 or above Upgrade to FortiNAC-F version 7.6.6 or above Upgrade to FortiSwitchManager version 7.2.9 or above Upgrade to FortiSwitchManager version 7.0.8 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](#)