CVE-2026-24858

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

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

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

ntegrity

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

Vendor	Fortinet
Product	Multiple Products
Name	Fortinet Multiple Products Authentication Bypass Using an Alternate Path or Channel Vulnerability
Required Action	Apply mitigations per vendor instructions, follow applicable BOD 22-01 guidance for cloud services, or discontinue use of the product if mitigations are unavailable.
Notes	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: https://fortiguard.fortinet.com/psirt/FG-IR-26-060 ; https://www.fortinet.com/blog/psirt-blogs/analysis-of-sso-abuse-on-fortios ; https://nvd.nist.gov/vuln/detail/CVE-2026-24858

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	FortiProxy	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	Ta
fortiguard.fortinet.com/psirt/FG-IR-26-060	psirt@fortinet.com	fortiguard.fortinet.com	Ve
www.cisa.gov/known-exploited-vulnerabilities-catalog	134c704f-9b21-4f2e-91b3-4a467353bcc0	www.cisa.gov	US
cert-portal.siemens.com/productcert/html/ssa-975644.html	0b142b55-0307-4c5a-b3c9-f314f3fb7c5e	cert-portal.siemens.com	Th
www.fortinet.com/blog/psirt-blogs/analysis-of-sso-abuse-on-fortios	134c704f-9b21-4f2e-91b3-4a467353bcc0	www.fortinet.com	Mi
CVE Program record	CVE.ORG	www.cve.org	ca
NVD vulnerability detail	NVD	nvd.nist.gov	ca
CISA Known Exploited Vulnerabilities catalog	CISA	www.cisa.gov	ke

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.

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status **status.cve.report**