CVE-2024-26009

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

Summary

CVE	CVE-2024-26009
State	PUBLISHED
Assigner	fortinet
Source Priority	CVE Program / NVD first with legacy fallback
Published	2025-08-12 19:15:27 UTC
Updated	2026-04-20 09:16:08 UTC
Description	An authentication bypass using an alternate path or channel [CWE-288] vulnerability in Fortinet FortiOS 6.4.0 through 6.4.1

Risk And Classification

Primary CVSS: v3.1 8.1 HIGH from nvd@nist.gov

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

Problem Types: CWE-288 | CWE-288 Execute unauthorized code or commands

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Primary	8.1	HIGH	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H
3.1	psirt@fortinet.com	Secondary	8.1	HIGH	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H
3.1	CNA	CVSS	7.9	HIGH	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:F/RL:O/RC:C

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

High

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

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

NVD Known Affected Configurations (CPE 2.3)

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Fortinet	FortiProxy	affected 7.4.0 7.4.2 semver	Not specified
CNA	Fortinet	FortiProxy	affected 7.2.0 7.2.8 semver	Not specified
CNA	Fortinet	FortiProxy	affected 7.0.0 7.0.15 semver	Not specified
CNA	Fortinet	FortiOS	affected 6.4.0 6.4.15 semver	Not specified
CNA	Fortinet	FortiOS	affected 6.2.0 6.2.16 semver	Not specified
CNA	Fortinet	FortiOS	affected 6.0.0 6.0.18 semver	Not specified
CNA	Fortinet	FortiPAM	affected 1.2.0	Not specified
CNA	Fortinet	FortiPAM	affected 1.1.0 1.1.2 semver	Not specified
CNA	Fortinet	FortiPAM	affected 1.0.0 1.0.3 semver	Not specified
CNA	Fortinet	FortiSwitchManager	affected 7.2.0 7.2.3 semver	Not specified
CNA	Fortinet	FortiSwitchManager	affected 7.0.0 7.0.3 semver	Not specified

References

Reference	Source	Link	Tags
fortiguard.fortinet.com/psirt/FG-IR-24-042	psirt@fortinet.com	fortiguard.fortinet.com	Vendor Advisory
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

Additional Advisory Data

Solutions

CNA: Upgrade to FortiSwitchManager version 7.2.4 or above Upgrade to FortiSwitchManager version 7.0.4 or above Upgrade to FortiOS version 6.4.16 or above Upgrade to FortiOS version 6.2.17 or above Upgrade to FortiManager version 7.0.12 or above Upgrade to FortiManager version 6.4.15 or above Upgrade to FortiPAM version 1.3.0 or above Upgrade to FortiProxy version 7.4.3 or above Upgrade to FortiProxy version 7.2.9 or above Upgrade to

FortiProxy version 7.0.16 or above

There are currently no legacy QID mappings associated with this CVE.