# CVE-2025-64157

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

## Summary

| | |
|---|---|
| **CVE** | CVE-2025-64157 |
| **State** | PUBLISHED |
| **Assigner** | fortinet |
| **Source Priority** | CVE Program / NVD first with legacy fallback |
| **Published** | 2026-02-10 16:16:09 UTC |
| **Updated** | 2026-05-12 13:17:23 UTC |
| **Description** | A use of externally-controlled format string vulnerability in Fortinet FortiOS 7.6.0 through 7.6.4, FortiOS 7.4.0 through 7.4.9, |

## Risk And Classification

**Primary CVSS:** v3.1 7.2 HIGH from nvd@nist.gov

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

**Problem Types:** CWE-134 | CWE-134 Execute unauthorized code or commands

| Version | Source | Type | Score | Severity | Vector |
|---|---|---|---|---|---|
| 3.1 | nvd@nist.gov | Primary | 7.2 | HIGH | CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H |
| 3.1 | psirt@fortinet.com | Secondary | 6.7 | MEDIUM | CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H |
| 3.1 | CNA | CVSS | 6.7 | MEDIUM | CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H/E:X/RL:X/RC:X |

## CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

High

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

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

## NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|---|---|---|---|---|---|---|
| Operating System | Fortinet | Fortios | All | All | All | All |

## Vendor Declared Affected Products

| Source | Vendor | Product | Version | Platforms |
|---|---|---|---|---|
| CNA | Fortinet | FortiOS | affected 7.6.0 7.6.4 semver | Not specified |
| CNA | Fortinet | FortiOS | affected 7.4.0 7.4.9 semver | Not specified |
| CNA | Fortinet | FortiOS | affected 7.2.0 7.2.11 semver | Not specified |
| CNA | Fortinet | FortiOS | affected 7.0.0 7.0.19 semver | Not specified |
| ADP | Siemens | RUGGEDCOM APE1808 | affected * custom | Not specified |

## References

| Reference | Source | Link | Tags |
|---|---|---|---|
| fortiguard.fortinet.com/psirt/FG-IR-25-795 | psirt@fortinet.com | fortiguard.fortinet.com | Vendor Ad |
| cert-portal.siemens.com/productcert/html/ssa-975644.html | 0b142b55-0307-4c5a-b3c9-f314f3fb7c5e | cert-portal.siemens.com | |
| CVE Program record | CVE.ORG | www.cve.org | canonical |
| NVD vulnerability detail | NVD | nvd.nist.gov | canonical, |

No vendor comments have been submitted for this CVE.

## Additional Advisory Data

Solutions

**CNA:** Upgrade to FortiOS version 7.6.5 or above Upgrade to FortiOS version 7.4.10 or above Upgrade to FortiProxy version 7.6.5 or above Upgrade to FortiPAM version 1.7.2 or above Upgrade to FortiSwitchManager version 7.2.8 or above Fortinet remediated this issue in FortiSASE version 25.4.c (not released) and hence customers do not need to perform any action.

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**