



CVE-2025-55018

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

Summary

CVE	CVE-2025-55018
State	PUBLISHED
Assigner	fortinet
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-02-10 16:16:08 UTC
Updated	2026-05-12 13:17:22 UTC
Description	An inconsistent interpretation of http requests ('http request smuggling') vulnerability in Fortinet FortiOS 7.6.0, FortiOS 7.4.0

Risk And Classification

Primary CVSS: v3.1 5.8 MEDIUM from psirt@fortinet.com

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

EPSS: 0.000800000 probability, percentile 0.234650000 (date 2026-05-12)

Problem Types: CWE-444 | CWE-444 Execute unauthorized code or commands

Version	Source	Type	Score	Severity	Vector
3.1	psirt@fortinet.com	Secondary	5.8	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:L/A:N
3.1	CNA	CVSS	5.2	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:L/A:N/E:P/RL:O/RC:C

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Changed

Confidentiality

None

Integrity

Low

CVSS

Availability

None

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Fortinet	Fortios	All	All	All	All
Operating System	Fortinet	Fortios	7.6.0	All	All	All
Operating System	Fortinet	Fortios	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Fortinet	FortiOS	affected 7.6.0	Not specified
CNA	Fortinet	FortiOS	affected 7.4.0 7.4.9 semver	Not specified
CNA	Fortinet	FortiOS	affected 7.2.0 7.2.13 semver	Not specified
CNA	Fortinet	FortiOS	affected 7.0.0 7.0.19 semver	Not specified
CNA	Fortinet	FortiOS	affected 6.4.3 6.4.16 semver	Not specified
ADP	Siemens	RUGGEDCOM APE1808	affected * custom	Not specified

References

Reference	Source	Link	Tags
fortiguard.fortinet.com/psirt/FG-IR-25-667	psirt@fortinet.com	fortiguard.fortinet.com	Vendor Ac
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 7.6.1 or above Upgrade to FortiOS version 7.4.10 or above

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

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