



CVE-2025-59809

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

Summary

CVE	CVE-2025-59809
State	PUBLISHED
Assigner	fortinet
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-14 16:16:31 UTC
Updated	2026-04-17 15:11:03 UTC
Description	A server-side request forgery (ssrf) vulnerability [CWE-918] vulnerability in Fortinet FortiSOAR PaaS 7.6.4, FortiSOAR Paa:

Risk And Classification

Primary CVSS: v3.1 4.3 MEDIUM from psirt@fortinet.com

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

EPSS: 0.000290000 probability, percentile 0.081590000 (date 2026-04-21)

Problem Types: CWE-918 | CWE-918 Information disclosure

Version	Source	Type	Score	Severity	Vector
3.1	psirt@fortinet.com	Secondary	4.3	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N
3.1	CNA	CVSS	4.1	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N/E:H/RL:O/RC:C

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

Low

Integrity

None

None

Availability

None

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Fortinet	FortiSOAR On-premise	affected 7.6.4	Not specified
CNA	Fortinet	FortiSOAR On-premise	affected 7.6.0 7.6.2 semver	Not specified
CNA	Fortinet	FortiSOAR On-premise	affected 7.5.0 7.5.2 semver	Not specified
CNA	Fortinet	FortiSOAR On-premise	affected 7.4.0 7.4.5 semver	Not specified
CNA	Fortinet	FortiSOAR On-premise	affected 7.3.0 7.3.3 semver	Not specified
CNA	Fortinet	FortiSOAR PaaS	affected 7.6.4	Not specified
CNA	Fortinet	FortiSOAR PaaS	affected 7.6.0 7.6.2 semver	Not specified
CNA	Fortinet	FortiSOAR PaaS	affected 7.5.0 7.5.2 semver	Not specified
CNA	Fortinet	FortiSOAR PaaS	affected 7.4.0 7.4.5 semver	Not specified
CNA	Fortinet	FortiSOAR PaaS	affected 7.3.0 7.3.3 semver	Not specified

References

Reference	Source	Link	Tags
fortiguard.fortinet.com/psirt/FG-IR-26-103	psirt@fortinet.com	fortiguard.fortinet.com	
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 FortiSOAR on-premise version 7.6.5 or above Upgrade to FortiSOAR on-premise version 7.6.3 or above Upgrade to upcoming FortiSOAR on-premise version 7.5.3 or above Upgrade to FortiSOAR PaaS version 7.6.5 or above Upgrade to FortiSOAR PaaS version 7.6.3 or above Upgrade to upcoming FortiSOAR PaaS version 7.5.3 or above

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

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