CVE-2025-61886

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

Summary

CVE	CVE-2025-61886
State	PUBLISHED
Assigner	fortinet
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-14 16:16:31 UTC
Updated	2026-04-22 19:09:04 UTC
Description	An Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability [CWE-79] vulnerability

Risk And Classification

Primary CVSS: v3.1 5.4 MEDIUM from psirt@fortinet.com

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

EPSS: 0.000320000 probability, percentile 0.092430000 (date 2026-04-22)

Problem Types: CWE-79 | CWE-79 Execute unauthorized code or commands

Version	Source	Type	Score	Severity	Vector
3.1	psirt@fortinet.com	Secondary	5.4	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N
3.1	CNA	CVSS	4.9	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/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

Required

Scope

Unchanged

Confidentiality

Low

Integrity

Low

Availability

None

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Fortinet	Fortisandbox	All	All	All	All
Application	Fortinet	Fortisandbox Cloud	5.0.4	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Fortinet	FortiSandbox PaaS	affected 5.0.0 5.0.4 semver	Not specified
CNA	Fortinet	FortiSandbox	affected 5.0.0 5.0.4 semver	Not specified

References

Reference	Source	Link	Tags
fortiguard.fortinet.com/psirt/FG-IR-26-109	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 FortiSandbox PaaS version 5.0.5 or above Upgrade to FortiSandbox version 5.0.5 or above

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