CVE-2026-26083

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

Summary

CVE	CVE-2026-26083
State	PUBLISHED
Assigner	fortinet
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-05-12 18:16:39 UTC
Updated	2026-05-12 18:57:02 UTC
Description	A missing authorization vulnerability in Fortinet FortiSandbox 5.0.0 through 5.0.1, FortiSandbox 4.4.0 through 4.4.8, FortiSa

Risk And Classification

Primary CVSS: v3.1 9.8 CRITICAL from psirt@fortinet.com

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

Problem Types: CWE-862 | CWE-862 Execute unauthorized code or commands

Version	Source	Type	Score	Severity	Vector
3.1	psirt@fortinet.com	Secondary	9.8	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
3.1	CNA	CVSS	9.1	CRITICAL	CVSS:3.1/AV:N/AC:L/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
Low

Privileges Required
None

User Interaction
None

Scope
Unchanged

Confidentiality
High

Integrity
High

Availability

High

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Fortinet	FortiSandbox Cloud	affected 5.0.0 5.0.1 semver	Not specified
CNA	Fortinet	FortiSandbox Cloud	affected 4.4.5 4.4.8 semver	Not specified
CNA	Fortinet	FortiSandbox	affected 5.0.0 5.0.1 semver	Not specified
CNA	Fortinet	FortiSandbox	affected 4.4.0 4.4.8 semver	Not specified
CNA	Fortinet	FortiSandbox	affected 4.2.1 4.2.8 semver	Not specified
CNA	Fortinet	FortiSandbox PaaS	affected 23.4.4374	Not specified
CNA	Fortinet	FortiSandbox PaaS	affected 23.4.4350	Not specified
CNA	Fortinet	FortiSandbox PaaS	affected 23.3.4329	Not specified
CNA	Fortinet	FortiSandbox PaaS	affected 23.1.4245	Not specified
CNA	Fortinet	FortiSandbox PaaS	affected 22.2.4151	Not specified
CNA	Fortinet	FortiSandbox PaaS	affected 22.2.4134	Not specified
CNA	Fortinet	FortiSandbox PaaS	affected 22.1.4113	Not specified
CNA	Fortinet	FortiSandbox PaaS	affected 21.4.4072	Not specified
CNA	Fortinet	FortiSandbox PaaS	affected 21.3.4055	Not specified
CNA	Fortinet	FortiSandbox PaaS	affected 5.0.0 5.0.1 semver	Not specified
CNA	Fortinet	FortiSandbox PaaS	affected 4.4.5 4.4.8 semver	Not specified

References

Reference	Source	Link	Tags
fortiguard.fortinet.com/psirt/FG-IR-26-136	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: Fortinet remediated this issue in FortiSandbox Cloud version 5.0.2 and hence customers do not need to perform any action. Fortinet remediated this issue in FortiSandbox Cloud version 4.4.9 and hence customers do not need to perform any action. Upgrade to FortiSandbox version 5.0.2 or above Upgrade to FortiSandbox version 4.4.9 or above

Upgrade to FortiSandbox PaaS version 5.0.2 or above Upgrade to FortiSandbox PaaS version 4.4.9 or above

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