PSIRT

Path traversal in csfd daemon

IR Number	FG-IR-24-259
Published Date	Jan 14, 2025
Updated Date	Mar 20, 2025
Component	OTHERS
Severity	High
CVSSv3 Score	7.1
Impact	Escalation of privilege
CVE ID	CVE-2024-48884 CVE-2024-48885
Download	CVRF CSAF

This site uses cookies. Some are essential to the operation of the site; others help us improve the user experience. By continuing to use the site, you consent to the use of these cookies. To learn more about cookies, please read our privacy policy.

Accept

Version	Affected	Solution
FortiManager 7.6	7.6.0 through 7.6.1	Upgrade to 7.6.2 or above
FortiManager 7.4	7.4.1 through 7.4.3	Upgrade to 7.4.4 or above
FortiManager 7.2	Not affected	Not Applicable
FortiManager 7.0	Not affected	Not Applicable
FortiManager 6.4	Not affected	Not Applicable
FortiManager Cloud 7.4	7.4.1 through 7.4.3	Upgrade to 7.4.4 or above
FortiOS 7.6	7.6.0	Upgrade to 7.6.1 or above
FortiOS 7.4	7.4.0 through 7.4.4	Upgrade to 7.4.5 or above
FortiOS 7.2	7.2.0 through 7.2.9	Upgrade to 7.2.10 or above
FortiOS 7.0	7.0.0 through 7.0.15	Upgrade to 7.0.16 or above
FortiOS 6.4	6.4.0 through 6.4.15	Upgrade to 6.4.16 or above
FortiProxy 7.6	Not affected	Not Applicable
FortiProxy 7.4	7.4.0 through 7.4.5	Upgrade to 7.4.6 or above
FortiProxy 7.2	7.2.0 through 7.2.11	Upgrade to 7.2.12 or above
FortiProxy 7.0	7.0.0 through 7.0.18	Upgrade to 7.0.19 or above
FortiProxy 2.0	2.0 all versions	Migrate to a fixed release
FortiProxy 1.2	1.2 all versions	Migrate to a fixed release

This site uses cookies. Some are essential to the operation of the site; others help us improve the user experience. By continuing to use the site, you consent to the use of these cookies. To learn more about cookies, please read our privacy policy.

Version	Affected	Solution
FortiVoice 7.0	7.0.0 through 7.0.4	Upgrade to 7.0.5 or above
FortiVoice 6.4	6.4.0 through 6.4.9	Upgrade to 6.4.10 or above
FortiVoice 6.0	6.0 all versions	Migrate to a fixed release
FortiWeb 7.6	7.6.0	Upgrade to 7.6.1 or above
FortiWeb 7.4	7.4.0 through 7.4.4	Upgrade to 7.4.5 or above
FortiWeb 7.2	7.2 all versions	Migrate to a fixed release
FortiWeb 7.0	7.0 all versions	Migrate to a fixed release
FortiWeb 6.4	6.4 all versions	Migrate to a fixed release

Follow the recommended upgrade path using our tool at: https://docs.fortinet.com/upgrade-tool

Fortinet in Q4/24 has remediated this issue in FortiSASE version 24.3.c and hence the customers need not perform any action.

Workarround :
disable the security fabric :

config system csf
set status disable
end

or
remove **fabric** from config system interface:

config system interface
edit "portY"

This site uses cookies. Some are essential to the operation of the site; others help us improve the user experience. By continuing to use the site, you consent to the use of these cookies. To learn more about cookies, please read our privacy policy.

Timeline

2025-01-14: Initial publication
2025-01-16: add workarounds
2025-03-20: added FortiOS 6.4.16 in fixed versions

Contact Us | Legal | Privacy | Partners | Feedback

Copyright © 2026 Fortinet, Inc. All Rights Reserved.

This site uses cookies. Some are essential to the operation of the site; others help us improve the user experience. By continuing to use the site, you consent to the use of these cookies. To learn more about cookies, please read our privacy policy.