PSIRT

No certificate name verification for fgfm connection

IR Number	FG-IR-24-046
Published Date	Apr 8, 2025
Component	OTHERS
Severity	⚠ High
CVSSv3 Score	7.1
Impact	Improper access control
CVE ID	CVE-2024-26013 CVE-2024-50565
CVRF	Download

Summary

A improper restriction of communication channel to intended endpoints vulnerability [CWE-923] in FortiOS, FortiProxy, FortiManager, FortiAnalyzer, FortiVoice and FortiWeb may allow an unauthenticated attacker in a man-in-the-middle position to impersonate the management device (FortiCloud server or/and in certain conditions, FortiManager), via intercepting the FGFM authentication request between the management device and the managed device

Version	Affected	Solution
FortiAnalyzer 7.6	Not affected	Not Applicable
FortiAnalyzer 7.4	7.4.0 through 7.4.2	Upgrade to 7.4.3 or above

Version	Affected	Solution
FortiAnalyzer 7.2	7.2.0 through 7.2.4	Upgrade to 7.2.5 or above
FortiAnalyzer 7.0	7.0.0 through 7.0.11	Upgrade to 7.0.12 or above
FortiAnalyzer 6.4	6.4.0 through 6.4.14	Upgrade to 6.4.15 or above
FortiAnalyzer 6.2	6.2.0 through 6.2.13	Upgrade to 6.2.14 or above
FortiManager 7.6	Not affected	Not Applicable
FortiManager 7.4	7.4.0 through 7.4.2	Upgrade to 7.4.3 or above
FortiManager 7.2	7.2.0 through 7.2.4	Upgrade to 7.2.5 or above
FortiManager 7.0	7.0.0 through 7.0.11	Upgrade to 7.0.12 or above
FortiManager 6.4	6.4.0 through 6.4.14	Upgrade to 6.4.15 or above
FortiManager 6.2	6.2.0 through 6.2.13	Upgrade to 6.2.14 or above
FortiOS 7.6	Not affected	Not Applicable
FortiOS 7.4	7.4.0 through 7.4.4	Upgrade to 7.4.5 or above
FortiOS 7.2	7.2.0 through 7.2.8	Upgrade to 7.2.9 or above
FortiOS 7.0	7.0.0 through 7.0.15	Upgrade to 7.0.16 or above
FortiOS 6.4	6.4 all versions	Migrate to a fixed release
FortiOS 6.2	6.2.0 through 6.2.16	Upgrade to 6.2.17 or above
FortiProxy 7.6	Not affected	Not Applicable
FortiProxy 7.4	7.4.0 through 7.4.2	Upgrade to 7.4.3 or above
FortiProxy 7.2	7.2.0 through 7.2.9	Upgrade to 7.2.10 or above
FortiProxy 7.0	7.0.0 through 7.0.15	Upgrade to 7.0.16 or above
FortiProxy 2.0	2.0 all versions	Migrate to a fixed release
FortiVoice 7.2	Not affected	Not Applicable
FortiVoice 7.0	7.0.0 through 7.0.2	Upgrade to 7.0.3 or above
FortiVoice 6.4	6.4.0 through 6.4.8	Upgrade to 6.4.9 or above
FortiVoice 6.0	6.0 all versions	Migrate to a fixed release

Version	Affected	Solution
FortiWeb 7.6	Not affected	Not Applicable
FortiWeb 7.4	7.4.0 through 7.4.2	Upgrade to 7.4.3 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

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

Acknowledgement

Internally discovered and reported by Théo Leleu of Fortinet Product Security team and Stephen Bevan of Fortinet Development team.

Timeline

2025-04-08: Initial publication