PSIRT

Missing Authentication for critical function in CAPWAP daemon

IR Number	FG-IR-26-125
Published Date	Apr 14, 2026
Component	OTHERS
Severity	⚠ Medium
Discovered	Internal
Attack Type	Unauthenticated
Known Exploited	No
CVSSv3 Score	6.2
Impact	Execute unauthorized code or commands
CVE ID	CVE-2025-53847

Version	Affected	Solution
FortiOS 7.6	7.6.0 through 7.6.3	Upgrade to 7.6.4 or above
FortiOS 7.4	7.4.0 through 7.4.8	Upgrade to 7.4.9 or above
FortiOS 7.2	7.2.0 through 7.2.11	Upgrade to 7.2.12 or above
FortiOS 7.0	7.0.0 through 7.0.17	Upgrade to 7.0.18 or above
FortiOS 6.4	6.4 all versions	Migrate to a fixed release
FortiOS 6.2	6.2.9 through 6.2.17	Migrate to a fixed release

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

Workaround :

Disable security fabric access into interface.
Only allow legit devices in `Wifi Controller > Managed FortiAPs`
Remove `inter-controller-peer` elements in `config wireless-controller inter-controller` configuration

Warning :

If `auto-auth-extension-device` is enabled in config system interface, any device can be authorized and then the vulnerability can be exploited without administrator authorization.
Please note that `auto-auth-extension-device` is disabled by default
If `inter-controller-peer` is set, it is strongly advised to change the `inter-controller-key` setting, even for fixed versions.