


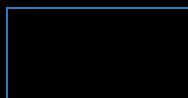




# Stack buffer overflow in CAPWAP daemon

IR Number	<b>FG-IR-25-632</b>
Published Date	<b>Nov 18, 2025</b>
Updated Date	<b>Nov 21, 2025</b>
Component	<b>OTHERS</b>
Severity	<b> Medium</b>
CVSSv3 Score	<b>6.9</b>
Impact	<b>Execute unauthorized code or commands</b>
CVE ID	<b>CVE-2025-58413</b>
Download	<b> CVRF</b> <b> CSAF</b>



<b>Version</b>	<b>Affected</b>	<b>Solution</b>
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 all versions	Migrate to a fixed release
FortiOS 7.0	7.0 all versions	Migrate to a fixed release
FortiOS 6.4	6.4 all versions	Migrate to a fixed release
FortiOS 6.2	6.2 all versions	Migrate to a fixed release
FortiOS 6.0	6.0 all versions	Migrate to a fixed release
FortiSASE 25.3	25.3.b	Fortinet remediated this issue in 25.3.c and hence customers do not need to perform any action.
FortiSASE 24.4	Not affected	Not Applicable
FortiSASE 23.3	Not affected	Not Applicable
FortiSASE 23.2	Not affected	Not Applicable

**Workarounds :**

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

## Acknowledgement

Internally discovered and reported by Gwendal Guégnaud of Fortinet Product Security team.

## Timeline

2025-11-18: Initial publication

2025-11-21: add workarounds

**FORTINET**®

[Contact Us](#) | [Legal](#) | [Privacy](#) | [Partners](#) | [Feedback](#)