Westermo-24-12: IbexOS Web Interface/WebAPI Session hijacking

CRITICAL / **HIGH** / MEDIUM / LOW 2024-09-25

Description

This security advisory describes a session hijacking vulnerability affecting a subset of the Westermo Ibex series.

Any authenticated user accessing the device through the Web Interface, WebAPI or CLI can hijack an open Web Interface or WebAPI session from another user. This means that an authenticated and logged-in user access can take over a session from another logged-in user and thereby potentially get full access to the device.

The requirements to exploit the vulnerability are:

- Another user is logged-in to the Web Interface or has an open session through the WebAPI
- The threat actor has valid credentials

Affected versions

Westermo Ibex series products running any of the following Ibex operating system versions are susceptible to the vulnerability:

- IbexOS 6.11.3
- IbexOS 6.11.4

Earlier versions are not affected.

Impact

Through the session replay attack an authenticated user can elevate its privilege and get the privilege to full access to the system.

In the case where *LDAP Authentication* is used, a user with valid credentials can spoof his identity, hijack a session and act as another, logged-in user.

Severity

Base score	The CVSS severity base score is 9.0.
Environmental	The CVSS severity environmental score is 8.0.
Vector string	CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:H/I:H/A:H/E:H/RL:O/RC:U/CR:H/IR:H/AR:H/MAV:N/MAC:L/MPR:L/MUI:R/MS:C/MC:H/MI:H/MA:H

Mitigation

We highly recommend upgrading to the latest IbexOS version **6.11.5**.

Workarounds to weaken the vulnerability:

- Disable access to the Web Interface, WebAPI and CLI
- Disable the user "monitor" by changing the password of the user “monitor” to a strong, random passphrase.
    - This does not prevent from spoofing the identity in case of *LDAP Authentication*
- Always log out from the Web Interface to destroy the open session which can be hijacked.
- Disable LDAP Authentication

References

- CAPEC - CAPEC-60: Reusing Session IDs (aka Session Replay) (Version 3.9) (mitre.org)

Revision History

Sept 25, 2024: Initial release