WESTERMO-21-01: Security Advisory

CRITICAL / HIGH / MEDIUM / LOW / INFORMATIONAL 2021-02-09

Security Vulnerability in SSH –
Incomplete validation of SSH username length

Description

WeOS releases in the range 4.19.0 - 4.28.5 and 5.6.0 - 5.9.2 are subject to a severe security vulnerability on units with SSH enabled. *Note: SSH is enabled by default on all interfaces in the factory configuration and for all new VLANs created.*

There is no limit to how long the SSH usernames can be. During arbitrary testing usernames exceeding 5000 characters were accepted and passed on to lower-layer authentication functions.

Extremely long usernames can cause resource starvation and be used in Denial-of-Service (DOS) attacks. The long usernames also appear in log files, which means they can be used to rapidly fill the logs and lose valuable audit trail information.

The vulnerability can for example be used in DOS attacks, but we cannot rule out that such long usernames do not cause other security problems, such as buffer overflows.

Customers with WeOS devices in the affected range are strongly recommended to immediately upgrade to the latest WeOS release.

Affected versions

- All versions from WeOS 4.19.0 to 4.28.5
- All versions from WeOS 5.6.0 to WeOS 5.9.2

Mitigation

There are several ways to mitigate this vulnerability.

- (Preferred) Upgrade to the latest WeOS release
  - WeOS 4 products: Upgrade to WeOS 4.28.6 or later
  - WeOS 5 products: Upgrade to WeOS 5.9.3 or later
- Upgrade to latest patch release of your currently installed WeOS version. Please see release notes for more information
- Disable SSH on all interfaces

References

Download WeOS 4.28.6 (zip, 87 MB)
Download WeOS 5.9.3 (zip, 44 MB)
Patch releases for earlier affected WeOS versions can be found in the WeOS firmware archive on the Westermo website.