Westermo-24-06: CVE-2021-36369 & CVE-2023-48795 - Vulnerability in SSH component of WeOS

Severity: **HIGH** 2024-11-11

Description

Two vulnerabilities in the SSH-component of WeOS can affect devices Westermo products:

1. CVE-2021-36369

"*Due to a non-RFC-compliant check of the available authentication methods in the client-side SSH code, it is possible for an SSH server to change the login process in its favor. This attack can bypass additional security measures such as FIDO2 tokens or SSH-Askpass. Thus, it allows an attacker to abuse a forwarded agent for logging on to another server unnoticed.*"

2. CVE-2023-48795

From Terrapin Attack (terrapin-attack.com):

" Terrapin is a prefix truncation attack targeting the SSH protocol. More precisely, Terrapin breaks the integrity of SSH's secure channel. By carefully adjusting the sequence numbers during the handshake, an attacker can remove an arbitrary amount of messages sent by the client or server at the beginning of the secure channel without the client or server noticing it."

Affected versions

Affects WeOS 5 to and including version 5.20.1

Affects WeOS 4 to and including version 4.33.2

Impact

The vulnerability could allow remote attackers to bypass integrity checks such that some packets are omitted (from the extension negotiation message), and a client and server may consequently end up with a connection for which some security features have been downgraded or disabled.

Severity

CVE-2021-36369

Base score	The CVSS severity base score is 7.5
Environmental	-
Vector string	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N

CVE-2021-48795

Base score	The CVSS severity base score is 5.9

Environmental	-
Vector string	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N

Mitigation

It's recommended to upgrade to WeO5 version as per below. The software is available for download at Westermo.

Workarounds

General recommendations that reduce but not eliminates risk associated with the above vulnerability:

- Limit administration access from external interfaces, by e.g. disable administrative access on outward facing interfaces
- Limit administration account access to trusted parties.
- Use best practices for passwords related to administration accounts.

Updates

The above-mentioned vulnerabilities have been removed in WeOS 5 version 5.22.0.

References

WeOS - Westermo Operating System ▷ Westermo https://www.westermo.com/solutions/weos

Terrapin-attack https://terrapin-attack.com/

CVE-2021-36369: Dropbear https://nvd.nist.gov/vuln/detail/CVE-2021-36369

CVE-2023-48795: Dropbear https://nvd.nist.gov/vuln/detail/CVE-2023-48795

Revision History

Nov 11, 2024: Initial release