Westermo-24-05: EDW-100 Security Advisory

Severity: **MEDIUM** 2024-05-28

Description

EDW-100 is a serial to Ethernet converter designed to allow RS-232, RS-422 and RS-485 serial devices to communicate via TCP/IP Ethernet networks.

Westermo acknowledges the following vulnerabilities that have been identified.

1. **Hidden root user with hardcoded password:** EDW-100 has a hidden root user account with a hardcoded password that cannot be changed, making EDW-100 vulnerable to unauthorized access (CWE-259: Use of Hard-coded Password, CWE-256: Plaintext Storage of a Password). This vulnerability has been assigned CVE-2024-36080.
2. **Unauthenticated users can read config containing password:** (CWE-522: Insufficiently Protected Credentials, CWE-256: Plaintext Storage of a Password) This vulnerability has been assigned CVE-2024-36081.

Affected versions

EDW-100 – All versions

Impact

EDW-100 is impacted as follows:

1. Hidden administrator account with hardcoded password. In the firmware package, in "image.bin", the username root and the password for this account are both hard-coded and exposed as strings that can trivially be extracted. Currently there is no way to change this password.
2. Unauthenticated user can read configuration-file containing password. An unauthenticated GET request can download the configuration-file that contains the configuration, including the username and passwords in clear-text.

Severity

Base score	The CVSS severity base score is 9.8
Environmental	The CVSS severity environmental score is 7.4
Vector string	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/MAV :L/MAC:H/MPR:N/MUI:N/MS:U

The CVSS Score was calculated using Common Vulnerability Scoring System Version 3.1 Calculator (first.org)

Mitigation

To mitigate the risks associated with these vulnerabilities, Westermo recommends network segregation, perimeter protection, network to network protection, and physical security measures.

EDW-100 functions as an industrial serial to ethernet converter. This means that EDW-100 does not in itself have any of the protective measures you require in a modern security posture, EDW-100 should not be placed at the edge of the network but instead deployed using the techniques mentioned in the IEC 62443 standard.

This means the use of network segregation and perimeter protection which can be accomplished by for example deploying a firewall and the use of VLANs.

If data needs to flow into, or out of, the security zone containing EDW-100 it is important to have network to network protection enabled which for example can be applied with a Virtual Private Network (VPN).

It is also crucial to have physical security measures put in place as the unit can be vulnerable to physical attacks and tampering. A recommendation to mitigate this risk is to place the unit in a separate enclosure with locks and alarms if it opened outside of normal maintenance.

While the unit's design characteristics may necessitate extra precautions, implementing the suggested countermeasures ensures a secure deployment that effectively addresses associated risks.

Replacement

Additionally, Westermo recommends replacing EDW-100 with Lynx DSS L105-S1. For further reference see 5-Port Managed Industrial Device Server Switch | L105-S1 ⊳ Westermo.

References

CWE - CWE-259: Use of Hard-coded Password (4.14) (mitre.org)

CWE - CWE-256: Plaintext Storage of a Password (4.14) (mitre.org)

CWE - CWE-522: Insufficiently Protected Credentials (4.14) (mitre.org)

Credits

Westermo thanks Nicolai Grødum and Sofia Lindqvist of PWC Norway for identifying and reporting these vulnerabilities.

Revision History

May 03, 2024: Initial release
May 28, 2024: Revision 1