

Westermo-25-06: Multiple vulnerabilities in EDW-100 & EDW-120

Severity: **HIGH**

2025-06-23

Description & Impact

EDW-100 and EDW-120 are serial to Ethernet converters 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. **CVE-2014-9222:** Affected units utilize a third-party component, AllegroSoft RomPagerⁱ, that have an identified vulnerability. A crafted http-request could cause denial of service.
2. **CVE-2014-9223:** Affected units utilize a third-party component, AllegroSoft RomPager, that have an identified vulnerability. A crafted http-request could cause denial of service.

Affected versions

EDW-100 – All versions

EDW-120 – All versions

Severity

<i>Base score</i>	The CVSS severity base score is 10
<i>Environmental</i>	The CVSS severity environmental score is 7.5
<i>Vector string</i>	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H/MAV:A/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 and EDW-120 functions as industrial serial to ethernet converters. This means that the devices do not in itself have any of the protective measures you require in a modern security posture. The units 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 or EDW-120 it is important to have network to network protection enabled which for example can be applied with a Virtual Private Network (VPN).

While the unit's design characteristics may necessitate extra precautions, implementing the suggested countermeasures ensures a secure deployment that effectively addresses associated risks. Following these recommendations reduces the attack vector, on which the CVSS Environmental score is based.

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

[NVD - CVE-2014-9222](#)

[NVD - CVE-2014-9223](#)

[RomPager® | Embedded Web Server | Allegro Software](#)

Credits

Westermo thanks Volvo Construction Equipment for identifying and reporting these vulnerabilities.

Revision History

June 23, 2025: Initial release

ⁱ RomPager® is registered by Allegro Software