

Login Lockout Resets in ICX35

Date: 2026-10-28

Version: 1.0

Summary

ICX35 devices are affected by a vulnerability of the integrated module webpage. Due to the lockout mechanism's implementation in client-side JavaScript, the password security mechanism could be bypassed by deleting cookies.

The following vulnerability affects one or more versions of the products listed in the next section:

ID	Title / Description	Severity
CWE-307	Improper Restriction of Excessive Authentication Attempts	CVSS v3.1: 5.2
CWE-602	Client-Side Enforcement of Server-Side Security	CVSS v3.1: 5.2

Affected Products

Brand	Product Line	Affected Version(s)
ProSoft Technology	X35-HWC-A ICX35-HWC-E	V1.14.153 and prior

Mitigation

Customers are advised to upgrade their devices to version 1.14.158

Acknowledgments

We would like to thank Rustam Amin, Cybersecurity Researcher, for finding and reporting this issue.

For Help or Feedback

To view all Belden Security Advisories or to report suspected security vulnerabilities, go to

<https://www.belden.com/security>.

For technical support and other requests, please visit <https://www.belden.com/support/technical-product-support-main>.

Disclaimer

THE SECURITY ADVISORY, AND INFORMATION CONTAINED HEREIN, ARE PROVIDED ON AN "AS IS" BASIS AND DO NOT IMPLY ANY KIND OF GUARANTEE OR WARRANTY, INCLUDING THE WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR USE. YOUR USE OF THE ADVISORY, AND INFORMATION CONTAINED HEREIN, OR MATERIALS LINKED FROM THE ADVISORY, IS AT YOUR OWN RISK. INFORMATION IN THIS ADVISORY AND ANY RELATED COMMUNICATIONS IS BASED ON OUR KNOWLEDGE AT THE TIME OF PUBLICATION AND IS SUBJECT TO CHANGE WITHOUT NOTICE. BELDEN RESERVES THE RIGHT TO CHANGE OR UPDATE ADVISORIES AT ANY TIME.

Revisions

V1.0 2026-10-28 Security Advisory published.