Jackson vulnerability in Industrial HiVision

Date: June 6, 2018
Version: 1.0

Summary

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

ID	Title / Description	Severity
CVE-2017-7525	A deserialization flaw was discovered in the jackson-databind, which could allow an unauthenticated user to perform code execution.	CVSS v3.0: 8.8 (*)

(*) The CVSS score deviates from the score in the CVE because the default installation of Industrial HiVision is not vulnerable. Both web server and user management must be enabled by the user to exploit this vulnerability.

Affected Products

Brand	Product Line / Platform	Product	Version
Hirschmann	Network Management Software	Industrial HiVision	06.0.08 and lower 07.0.04 and lower 07.1.01 and lower

Solution

Updates are available which address the vulnerability. Customers are advised to update their products.

Brand	Product Line / Platform	Product	Version
Hirschmann	Network Management Software	Industrial HiVision	06.0.09 07.0.05 07.1.02

For Help or Feedback

To view all Belden Security Advisories and Bulletins or to report suspected security vulnerabilities, go to https://www.belden.com/security.
For technical support and other requests, please visit https://hirschmann-support.belden.com/.

Disclaimer

Revisions

V1.0 (June 6, 2018): Bulletin created.