Industrial HiVision: Opening of IHP project files may lead to automatic execution of arbitrary scripts or binaries

Date: 2023-03-28

Version: 1.0

Executive Summary

A vulnerability in the execution of user-configured scheduler actions may allow a local attacker to execute arbitrary scripts or binaries.

Details

Opening a manipulated IHP project file will cause that the scheduler of Industrial HiVision executes scripts or binaries out of the file as configured by the attacker without warning after a restart of Industrial HiVision.

Impact

A local attacker can execute malicious scripts or binaries with administrator privileges. This may lead to the loss of confidentiality, integrity, and availability.

CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H 7.8 (HIGH)

Affected Products

Brand	Product Line / Platform	Product	Version
Hirschmann	Network Management	Industrial HiVision	05.0.00 up to 08.3.01

Solution

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

Brand	Product Line / Platform	Product	Version
Hirschmann	Network Management	Industrial Hivision	08.3.02 or higher

For Help or Feedback

To view all Belden Security 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

THE SECURITY BULLETIN, 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 BULLETIN, AND INFORMATION CONTAINED HEREIN, OR MATERIALS LINKED FROM THE BULLETIN, IS AT YOUR OWN RISK. INFORMATION IN THIS BULLETIN 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 BULLETINS AT ANY TIME.

Revisions

V1.0 (2023-03-28):	Bulletin published.