Industrial HiVision: Configured external applications may lead to execution of arbitrary binaries

Date: 2022-10-17
Version: 1.0

Executive Summary

A bug in the execution of user-configured external applications may allow a local attacker to execute arbitrary binaries.

Details

A local attacker may place a malicious binary in the path of a user-configured external application. The path needs to contain at least one whitespace for a successful exploitation. Due to insufficient path sanitization an attacker-placed binary is executed instead of the intended external application.

Depending on the type of the external application it is either run with the privileges of the GUI user or with the privileges of the master service. The action associated with the configured external application must be triggered in order to exploit the vulnerability, e.g., ping of a managed device.

The CVSS v3.1 score is 7.3 (High): CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H

Impact

A local attacker can gain elevated privileges by inserting an arbitrary binary in the path of a configured external application.

Affected Products

Brand	Product Line / Platform	Product	Version
Hirschmann	Network Management	Industrial HiVision	08.1.03 or lower

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	08.1.04 or higher
Hirschmann	Network Management	Industrial HiVision	08.2.00 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

Revisions

V1.0 (2022-10-17):	Bulletin created.