Weaknesses in Hirschmann Classic Platform switches when using plaintext HTTP for remote management access

Date: March 08, 2018
Version: 1.1
References: ICSA-18-065-01

Executive Summary

Hirschmann Classic Platform switches have multiple weaknesses when using plaintext HTTP for remote management access.

Details

Remote device management over plaintext HTTP connections, which is enabled by default, is susceptible to the following weaknesses:

1. Session fixation (CWE-384)
2. Information exposure through query strings (CWE-598, CWE-200)
3. Cleartext transmission of sensitive information (CWE-319)
4. Use reversible encryption algorithm for password (CWE-326, CWE-327)

Impact

The weaknesses may result in a loss of confidentiality and integrity of data passing between the management station and the impacted product, i.e. man-in-the-middle attack to read and modify configuration data.

Affected Products

Brand	Product Line / Platform	Product	Version
Hirschmann	Classic	RS, RSR, RSB, MACH100, MACH1000, MACH4000, MS, OCTOPUS	All versions

Solution

We strongly recommend customers to:

- Disable HTTP for remote management access
- Use the secure HTTPS or SSH protocols for remote management access
- Use the “Restricted Management Access” feature to restrict access to known IP addresses

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.eu.com.

Acknowledgments

Belden thanks the following for working with us to help protect customers:

- Ilya Karpov, Evgeniy Druzhinin, Damir Zainullin, Mikhail Tsvetkov from Positive Technologies

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 (February 23, 2018):	Bulletin created.
V1.1 (March 08, 2018):	Updated references.