Weaknesses in Hirschmann Classic Platform switches in the user authentication module

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

Executive Summary

Hirschmann Classic Platform switches have two weaknesses in the user authentication module.

Details

The user authentication module is susceptible to the following weaknesses:

1. Use of hardcoded user name (CWE-200)
2. Improper restriction of excessive authentication attempts (CWE-307)

Impact

The weaknesses may allow attackers to brute force user accounts in order to gain access to the device.

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 restrict access to remote management access. Following mitigation strategies might be applied:

- Use of complex user passwords
- Use the “Restricted Management Access” feature to restrict access to known IP addresses
- Disable remote management access when not in use

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

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.