

Restricted user roles may gain write access to devices managed by Industrial HiVision

Date: January 06, 2017

Version: 1.0

References: -

Executive Summary

Users with restricted (read-only) access may gain write access to devices managed by Industrial HiVision.

Details

Industrial HiVision allows administrators to restrict user access through its User Management feature. The Access Role with 'Login' permission should allow read-only access and prevent write access to any device managed in the software. Nevertheless, such a user can use MultiConfig™ to change certain parameters and then view the stored credentials of a device. With these credentials, the user may then also gain write access to the device, e.g. by using the web-based interface of the device or an SNMP Browser.

Impact

Possible write access to devices managed by Industrial HiVision.

Affected Products

Brand	Product Line / Platform	Product	Version
Hirschmann	Network Management	Industrial HiVision	06.0.00 - 06.0.05, 07.0.00

Solution

Updates are available which restrict the 'Login' role as expected.

Brand	Product Line / Platform	Product	Version
Hirschmann	Network Management	Industrial HiVision	06.0.06, 07.0.01

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>.

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 (January 06, 2017): Bulletin published.