

### Belden Security Bulletin – Industrial IT BSECV-2017-15

# Web Server Authentication Bypass Vulnerability in HiOS and HiSecOS

Date: May 25, 2018

Version: 1.0

#### **Executive Summary**

A vulnerability in the HTTP(S) management module of HiOS and HiSecOS devices could allow an unauthenticated, remote attacker to bypass authentication for web server resources, such as password protected upload/download pages.

#### **Details**

The vulnerability is due to improper handling of authentication requests. An attacker could exploit this vulnerability by crafting specially formed HTTP requests and incorrectly receive the authentication status and privilege of a previously authenticated user. A CVSSv3 score of 8.1 (High) was calculated for this vulnerability.

#### **Impact**

An exploit could allow the attacker to execute administrative actions like configuration download/upload, changing the firmware or gain administrative access to the device.

#### Affected Products

Brand	Product Line / Platform	Product	Version
Hirschmann	HiOS	RSP, RSPE, RSPS,	05.0.07 and lower
		RSPL, MSP, EES,	06.1.04 and lower
		EESX, GRS, OS, RED	06.2.00
	HiSecOS	EAGLE	03.0.02 and lower

#### Solution

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

Brand	Product Line / Platform	Product	Version
Hirschmann	HiOS	RSP, RSPE, RSPS,	06.1.05
		RSPL, MSP, EES, EESX, GRS, OS, RED	07.0.00
	HiSecOS	EAGLE	03.0.03
			03.1.00

#### For Help or Feedback

To view all Belden Security Advisories and Bulletins or to report suspected security vulnerabilities, go to <a href="https://www.belden.com/security">https://www.belden.com/security</a>.

For technical support and other requests, please visit <a href="https://hirschmann-support.belden.eu.com">https://hirschmann-support.belden.eu.com</a>.

#### **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



## Belden Security Bulletin – Industrial IT BSECV-2017-15

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 (May 25, 2018): Bulletin created.

BSECV-2017-15 ©Belden Inc. 2018 Page 2 of 2