Web Server Buffer Overflow in HiOS and HiSecOS products

Date: 2020-03-24
Version: 1.2
References: CVE-2020-6994[1]

Executive Summary

A vulnerability in the HTTP(S) web server of HiOS and HiSecOS devices could allow an unauthenticated, remote attacker to overflow a buffer and fully compromise the target device.

Details

The vulnerability is due to improper parsing of URL arguments. An attacker could exploit this vulnerability by crafting specially formed HTTP requests and overflow an internal buffer. A CVSSv3 score of 9.8 (Critical)[2] was calculated for this vulnerability.

Impact

An exploit could allow the attacker to execute arbitrary code which leads to a full compromise of the target device.

Affected Products

Brand	Product Line / Platform	Product	Version
Hirschmann	HiOS	RSP, RSPE, RSPS, RSPL, MSP, EES, EESX, GRS, OS, RED	07.0.02 or lower
Hirschmann	HiSecOS	EAGLE20/30	03.2.00 or lower

Solution

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

Brand	Product Line / Platform	Product	Version
Hirschmann	HiOS	RSP, RSPE, RSPS, RSPL, MSP, EES, EESX, GRS, OS, RED	07.0.03 or higher
Hirschmann	HiSecOS	EAGLE20/30	03.3.00 or higher

As a workaround, we strongly recommend customers to either use the “IP Access Restriction” feature to restrict HTTP and HTTPS to trusted IP addresses or disable the HTTP and HTTPS server.

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.com.

Acknowledgments

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

- Sebastian Krause, Senior Security Consultant, GAI NetConsult GmbH
- Toralf Gimpel, Senior Security Consultant, GAI NetConsult GmbH

Related Links

- [1] https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-6994
- [2] https://www.first.org/cvss/calculator/3.0#CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

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 (2020-02-14):	Bulletin created.
V1.1 (2020-02-26):	Update solution and include workaround.
V1.2 (2020-03-24):	Include CVE identifier and URL.