Password Change Authentication Bypass Vulnerability in HiOS & HiSecOS

Date: 2021-05-11
Version: 1.0
References: CVE-2021-27734

Executive Summary
Under some conditions, the HTTP(S) server does not correctly check whether a request to change a password is properly authenticated.

Details
The CVSS v3.1 severity of this vulnerability is 9.8 (critical):

Impact
An attacker may change the password of any existing user.

Affected Products

<table>
<thead>
<tr>
<th>Brand</th>
<th>Product Line / Platform</th>
<th>Product</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hirschmann</td>
<td>HiOS</td>
<td>RSP, RSPE, RSPS, RSPL, MSP, EES, EESX, GRS, OS, RED</td>
<td>07.1.01, 07.1.02, 08.1.00 – 08.5.xx</td>
</tr>
<tr>
<td>Hirschmann</td>
<td>HiSecOS</td>
<td>EAGLE</td>
<td>03.3.00 or higher</td>
</tr>
</tbody>
</table>

Solution
Updates are available, which address the vulnerability. Customers are advised to update their product as soon as possible.

<table>
<thead>
<tr>
<th>Brand</th>
<th>Product Line / Platform</th>
<th>Product</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hirschmann</td>
<td>HiOS</td>
<td>RSP, RSPE, RSPS, RSPL, MSP, EES, EESX, GRS, OS, RED</td>
<td>07.1.03 or higher, 08.6.00 or higher</td>
</tr>
<tr>
<td>Hirschmann</td>
<td>HiSecOS</td>
<td>EAGLE</td>
<td>04.1.00 or higher</td>
</tr>
</tbody>
</table>

Mitigation: Turn off the HTTP and HTTPS server or restrict access to both protocols to trusted IP addresses via the Restricted Management Access feature.

For Help or Feedback
To view all Belden Security 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.

Related Links

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