Security Advisory MRSA-2022-0801: Software vulnerability in ETOS/ISM SW 3-3

Version 1.11 - 19.01.2024

Summary

Several vulnerabilities have been identified in the SW 3-3 assembly of ETOS® and further ISM® based products:

An attacker could exploit a vulnerability in the webserver by crafting a special HTTP request message to fully compromise the target device. The vulnerability documented in CVE-2020-6994 is classified with a CVSS score of 9.8 (critical)[1] and described in BSECV-2020-01[2].

Several vulnerabilities in the XML parser of the device have been identified. An attacker could exploit these vulnerabilities by uploading a specially crafted XML file to fully compromise the device. The vulnerabilities documented in CVE-2022-40674[7] and CVE-2022-43680[8] are classified with a CVSS score of 9.8(critical) and 7.5 (high) and described in BSECV-2022-26[6].

Further vulnerabilities targeting the XML parser are: CVE-2021-45960[10], CVE-2021-46143[11], CVE-2022-22822[12], CVE-2022-22823[13], CVE-2022-22824[14], CVE-2022-22825[15], CVE-2022-22826[16], CVE-2022-22827[17], CVE-2022-25314[18], CVE-2022-25315[19], CVE-2022-25235[20], CVE-2022-25236[21], CVE-2022-23852[22] and CVE-2022-23990[23] documented in BSECV-2022-07[9] with a CVSS score between 7.5 (high) and 9.8 (critical).

Maschinenfabrik Reinhausen GmbH provides its customers with products of high quality and therefore this Security Advisory shall inform you about status and possible remediation.

Products

Products:	ETOS/ISM – all versions
Product assembly:	SW 3-3
Vulnerable:	SW 3-3-Hirschmann PRP and HSR (HiOS) Software 07.1.07 and lower
Recommended:	HiOS Software 07.1.08 and higher - addressing all vulnerabilities. It can be downloaded from: https://hirschmann-support.belden.com/en/downloads/files/web-ees-07108zip. Please note: use the file, which contains PRP for the SW3-3, here: HiOS-EES-PRP-07108.bin

Description

Maschinenfabrik Reinhausen was informed of a vulnerability report that affects the SW 3-3 assembly of the ETOS® and ISM® series. The SW 3-3 assembly is included if the Parallel Redundancy Protocol (PRP) or High-availability Seamless Redundancy (HSR) is ordered. The SW 3-3 assembly is based on the Belden/Hirschmann EES-25 ethernet switch.

To successfully exploit these software vulnerabilities an attacker must inject specifically formatted code into the web interface of the switch, which then leads to unauthorized network connections, download of possibly malicious codes and subsequent execution. The impact results in a loss of availability of the system as well as confidentiality and integrity of stored information on the vulnerable system. This could be used to steal login credentials, raise local privileges or perform lateral movement and compromise of further systems.

Further analysis of the vulnerability is available from Belden[2][6], CISA[3] and BSI[4].

Updates to software versions that are not vulnerable are strongly recommended in a timely manner. The mitigations listed below are available until the system software can be updated.

No known public exploits specifically target this vulnerability are known at this point of time.

Software Updates

Software Updates are available via the following links:

- The recommended update can be downloaded by this link: https://hirschmann-support.belden.com/en/downloads/files/web-ees-07108zip. Please note, a registration is required prior downloading and use the file, which contains PRP in its name for the SW3-3, here: HiOS-EES-PRP-07108.bin

- In general, software updates for SW-3-3 are available via the EES25-Website: https://catalog.belden.com/index.cfm?event=pd&p=PF_942050003
  -> Downloads -> Software File -> Software EES -> Download

- Security Bulletins: https://www.belden.com/support/security-assurance
  -> Search the page for the term “HiOS”, as this is the operating system of the SW3-3, using the browser’s search engine

For updates and further information please refer to the manufacturer Belden and the product EES-25.

For further instructions regarding the ETOS® / ISM® SW 3-3 assembly see section 8.1.23 “Configuring media converter with managed switch” of the ETOS® operating instructions[5].

Mitigations

The following mitigations are possible to lower the risk:

1. Keep software up to date.
2. Use the “IP Access Restriction” feature to restrict HTTP and HTTPS to trusted IP addresses only
3. Disable the HTTP and HTTPS server. Management is still possible via SSH.

General recommendations on IT Security

- Ensure that only authorized personnel have access to the device.
- Only use the device within an ESP (electronic security perimeter). Do not connect the device to the Internet in an unprotected state. Use mechanisms for vertical and horizontal network segmentation and security gateways (firewalls) at the transition points.
- Ensure that the device is only operated by trained personnel who are familiar with IT security.
- Check regularly whether software updates are available for the device and perform the updates.

Change history

- 0.1: Start of draft on August 2nd, 2022. Add links for software updates and possible mitigations.
- 0.2: Add detailed information regarding SW 3-3 assembly.
- 0.3: Refer to ETOS® operating instructions, clarify SW 3-3 order with PRP, clarify product and software versions.
- 1.0: Released on August 9th 2022.
- 1.1: Minor wording changes on August 18th 2022.
- 1.2: Update link to ETOS® operating instructions [5] as of September 1st 2022.
- 1.3: SW 3-3 with the High-availability Seamless Redundancy (HSR) is also affected, added as of September 22nd 2022.
- 1.4: Improve instructions for download in “Software Updates”, added March 17th 2023.
- 1.5: Added information regarding expat vulnerabilities documented in CVE-2022-40674 and CVE-2022-43680, update section number in latest ETOS user manual. Update mitigation to use SSH for configuration if HTTP and HTTPS are disabled. Updated August 10th 2023.
- 1.6: Fix version number of recommended HiOS Software from 07.0.08 to 07.1.08. August 23rd 2023.
- 1.7: Adding BSECV references to CVEs, added libexpat CVEs and changed description to adress both HTTP buffer overflow and xml vulnerabilities. Added search description on the vendor page. October the 6th 2023.
- 1.8: Removed section “Products – available”, as Belden released HiOS 07.1.08. January 09th 20224.
- 1.9: Added download links to belden website. January 11th 2024.
- 1.10: Added information about PRP. January 19th 2024.
- 1.11: Review and release for publication. January 19th 2024.

Additional information

[1] National Vulnerability Database: CVE-2020-6994.
URL: https://nvd.nist.gov/vuln/detail/CVE-2020-6994/

[2] Belden Security Bulletin BSECV-2020-01.
URL: https://assets.belden.com/m/7aba5ef98b96f94/original/Security-Bulletin-Web-Server-Buffer-Overflow-HiOS-HiSecOS_BSECV-2020-01.pdf

[3] CISA Advisory: Hirschmann Automation and Control HiOS and HiSecOS Products.
URL: https://www.cisa.gov/uscert/ics/advisories/icsa-20-091-01

[4] BSI CSW-Nr. 2020-181608-11a3: Schwachstelle in Hirschmann Industrial-Ethernet-Produkten.
Not publicly available.

[5] ETOS® Operating instructions.
URL:
https://www.reinhausen.com/fileadmin/downloadcenter/products/transformer_automation/etos_all_variants/ba/7815063_en.pdf

[6] Belden Security Bulletin BSECV-2022-26.
URL: https://assets.belden.com/m/6f2d4e1f6bbaeb54/original/BSECV-2022-26.pdf

[7] National Vulnerability Database: CVE-2022-40674.
URL: https://nvd.nist.gov/vuln/detail/CVE-2022-40674/

[8] National Vulnerability Database: CVE-2022-40680.
URL: https://nvd.nist.gov/vuln/detail/CVE-2022-40680/

[9] Belden Security Bulletin BSECV-2022-07.
URL: https://assets.belden.com/m/5513203acb22e570/original/Belden_Security_Bulletin_BSECV-2022-07.pdf

[10] National Vulnerability Database: CVE-2021-45960.
URL: https://nvd.nist.gov/vuln/detail/CVE-2021-45960

[11] National Vulnerability Database: CVE-2021-46143.
URL: https://nvd.nist.gov/vuln/detail/CVE-2021-46143

[12] National Vulnerability Database: CVE-2022-22822.
URL: https://nvd.nist.gov/vuln/detail/CVE-2022-22822

[13] National Vulnerability Database: CVE-2022-22823.
URL: https://nvd.nist.gov/vuln/detail/CVE-2022-22823

[14] National Vulnerability Database: CVE-2022-22824.
URL: https://nvd.nist.gov/vuln/detail/CVE-2022-22824

[15] National Vulnerability Database: CVE-2022-22825.
URL: https://nvd.nist.gov/vuln/detail/CVE-2022-22825

[16] National Vulnerability Database: CVE-2022-22826.
URL: https://nvd.nist.gov/vuln/detail/CVE-2022-22826

[17] National Vulnerability Database: CVE-2022-22827.
URL: https://nvd.nist.gov/vuln/detail/CVE-2022-22827

[18] National Vulnerability Database: CVE-2022-25314.
URL: https://nvd.nist.gov/vuln/detail/CVE-2022-25314

[19] National Vulnerability Database: CVE-2022-25315.
URL: https://nvd.nist.gov/vuln/detail/CVE-2022-25315

[20] National Vulnerability Database: CVE-2022-25235.
URL: https://nvd.nist.gov/vuln/detail/CVE-2022-25235

[21] National Vulnerability Database: CVE-2022-25236.
URL: https://nvd.nist.gov/vuln/detail/CVE-2022-25236

[22] National Vulnerability Database: CVE-2022-23852.
URL: https://nvd.nist.gov/vuln/detail/CVE-2022-23852

[23] National Vulnerability Database: CVE-2022-23990.
URL: https://nvd.nist.gov/vuln/detail/CVE-2022-23990