MR Product CERT: ProductCERT@reinhausen.com

Security Advisory MRSA-2023-1001: Software vulnerability in ETOS®/ISM® - Broken Authorization

Version 1.0 - 14.12.2023

Summary

Some ETOS® systems, equipped with a specific PLC,do not properly check access permissions on several ETOS® operations within the web visualization and executes those a with a possible success rate.

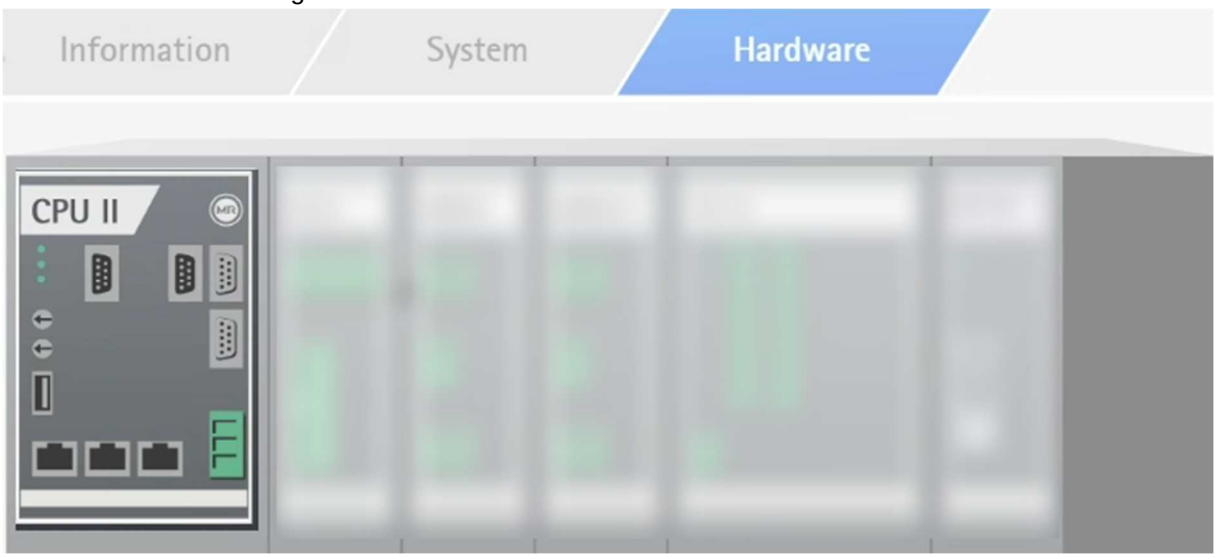
Products

Following products are affected:

- ETOS® with software versions up to 4.0.0, which do not have the hardware overview shown below

Following products are **generally not** affected:

- ETOS® with the following hardware overview:



Description

The vulnerability assumes a malicious actor who has advanced system knowledge and network access. The vulnerability allows such a malicious actor to bypass the existing access control in the web visualization to trigger several ETOS® operations although he has no permission to do so. Those operations get executed with an uninitialized user group, which may happen to be successful in some circumstances. Authentication is not required to successfully exploit this vulnerability. This vulnerability affects access to the ETOS® web interface, not SCADA interfaces.

Vulnerability classification

The classification of this vulnerability has been performed by using CVSS 3.1 (Common Vulnerability Scoring System Version 3.1 - http://www.first.org/cvss/). The score of this vulnerability is hereby defined by the base and environment score, where the recommended environment setup is considered.

A successful exploit for this vulnerability is not known to MR as of this date.

CVSS Score: 7.5 (High)

CVSS 3.1 Vector String:
https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:A/AC:H/PR:N/UI:N/S:U/C:L/I:H/A:H/CR:M/IR:H/AR:M

Software Updates

MR provides software updates addressing and fixing this vulnerability. Please refer to either https://portal.reinhausen.com or your local MR service manager.

The relevant fix is available in Version 4.0.1 and later.

Mitigations

The following mitigations are possible to lower the risk:

1. Restrict access to ETOS® to only trustworthy network addresses using an external firewall.

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 October 10th, 2023.
- 0.2: Content update on November 24th, 2023.
- 0.3: Minor language changes on November 24th, 2023.
- 0.4: Minor language changes on November 29th, 2023.
- 0.5: Addes screenshot of not affected device types on December 7th, 2023.
- 1.0: Minor wording changes and formatting improvements, finalize release on December 14th 2023.