SOCOMEC Security Notification

11 April 2025

Overview

Socomec has always been committed to building security into its products in order to guarantee the security of the installation or facility and to protect its users. Products evolve, and their design becomes more complex as it adds new technological layers such as electronics or IT.

Additionally, the functions and features provided to our customers become more generalised as they are no longer based on a single, stand-alone product, but on a complete “eco-system” comprising a set of products, communication networks and virtual servers in the Cloud and their associated applications.

To ensure a security along the system livecycle, Socomec strongly recommand to apply remediations as soon as possible, according your risk assessment.

Summary

A denial of service vulnerability exists in the Modbus RTU over TCP functionality of Socomec DIRIS Digiware M-70 1.6.9. A specially crafted network packet can lead to denial of service. An attacker can send an unauthenticated packet to trigger this vulnerability.

Affected Products and Versions

Product Version

Socomec DIRIS Digiware M-70 1.6.9 https://www.socomec.us/en-us/reference/48290222

Vulnerability Details

CVE ID: CVE-2025-23417

CVSS v3.1 Base Score 8.6 - CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:H

CWE-306 - Missing Authentication for Critical Function

The DIRIS Digiware M-50/M-70 gateway functions as the access point for industrial power monitoring systems, providing power supply and communication connection to devices in the electrical installation. It also includes a webserver WEBVIEW-M for the remote visualisation and analysis of measurements and consumption.

SOCOMEC SECURITY NOTIFICATION

The Socomec M-70 has a Modbus RTU over TCP service that is used by it's configuration software called Easy Config System. An attacker could send an unauthenticated packet using the Modbus RTU over TCP protcol to remotely factory reset the device resulting in a denial of service. Part of the factory reset procedure is to restore the documented default passwords for the M-70 webserver known as WEBVIEW-M. This would allow an attacker increased privileges as they could then access the WEBVIEW-M user accounts using the default passwords.

An attacker can trigger the factory reset mechanism by sending a Modbus RTU over TCP message through port 503 using the Write Single Register function code (6) to write the specific value 229 to register number 57856.

REMEDIATION

AFFECTED PRODUCT & VERSION	WORKAROUND
Socomec DIRIS Digiware M-70 1.6.9	Using the Cyber Security user profile in WEBVIEW-M, disable Modbus over Ethernet Writing. This change will disable writing over both ModbusTCP (port 502) and Modbus RTU over TCP (port 503).

REMEDIATION

To prevent the use of writing command by modbus, it is possibile to disable this feature.

The workaround, as explained in the user documentation, is to disable the writing modbus command.

The fix will be implemented in the next generation of this gateway, the modbus (read & write) will be disabled by default.

RELEASE DATES :

- Workaround already in place

- Fix in roughly 2 years

General Security Recommendations

We strongly recommend the following industry cybersecurity best practices.

- Locate control and safety system networks and remote devices behind firewalls and isolate them from the business network.
- Install physical controls so no unauthorized personnel can access your industrial control and safety systems, components, peripheral equipment, and networks.
- Place all controllers in locked cabinets and never leave them in the “Program” mode.
- Never connect programming software to any network other than the network for the devices that it is intended for.
- Scan all methods of mobile data exchange with the isolated network such as CDs, USB drives, etc. before use in the terminals or any node connected to these networks.
- Never allow mobile devices that have connected to any other network besides the intended network to connect to the safety or control networks without proper sanitation.
- Minimize network exposure for all control system devices and systems and ensure that they are not accessible from the Internet.
- When remote access is required, use secure methods, such as Virtual Private Networks (VPNs). Recognize that VPNs may have vulnerabilities and should be updated to the most current version available. Also, understand that VPNs are only as secure as the connected devices.

For more information refer to the Socomec Cybersecurity Best Practices document.

CONTACT US

This document provides an overview of the identified vulnerability or vulnerabilities and actions required to mitigate. For more details and assistance on how to protect your installation, contact your local Socomec Cybersecurity representative.

Need to report and incident or a vunerability ? HERE

For further information related to cybersecurity in Socomec’s products, visit the company’s cybersecurity support portal page HERE.

SOCOMEC SECURITY NOTIFICATION

LEGAL DISCLAIMER

SOCOMEC SECURITY NOTIFICATIONS AND ALL THE INFORMATION CONTAINED THEREIN ARE INTENDED TO INFORM ANY USER OF EQUIPMENT MARKETED BY THE SOCOMEC GROUP ("SOCOMEC") OF OPERATIONAL TECHNOLOGIES SECURITY VULNERABILITIES (THE "VULNERABILITIES") IDENTIFIED IN SAID EQUIPMENT, AS WELL AS TO COMMUNICATE (A) RECOMMENDATIONS TO LIMIT THE EFFECTS OF A VULNERABILITY, (B) MEASURES TO REMEDY A VULNERABILITY, OR (C) GENERAL SECURITY RECOMMENDATIONS. THIS INFORMATION IS PROVIDED AS IS, WITH NO KNOWLEDGE OF THE USER'S SITUATION AND WITHOUT ANY GUARANTEE WHATSOEVER, IN PARTICULAR AS TO ITS SUITABILITY FOR ANY PROBLEMS ENCOUNTERED BY THE USER.

IN NO EVENT SHALL SOCOMEC BE LIABLE FOR ANY DAMAGES OR LOSSES WHATSOEVER IN CONNECTION WITH A SECURITY NOTIFICATION, INCLUDING DIRECT, INDIRECT, INCIDENTAL, CONSEQUENTIAL, LOSS OF BUSINESS PROFITS OR SPECIAL DAMAGES, EVEN IF SOCOMEC HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. YOUR DECISION TO FOLLOW ANY RECOMMENDATION FROM A SECURITY NOTIFICATION IS AT YOUR OWN RISK, AND YOU ARE SOLELY LIABLE FOR ANY DAMAGES TO YOUR SYSTEMS OR ASSETS, OR OTHER LOSSES RESULTING FROM MEASURES YOU TAKE TO FOLLOW A RECOMMENDATION.

SOCOMEC RESERVES THE RIGHT TO UPDATE OR CHANGE THE CONTENT OF A SECURITY NOTIFICATION AT ANY TIME AND AT ITS SOLE DISCRETION.

IF YOU THINK YOU MAY BE AFFECTED BY A VULNERABILITY IN YOUR SOCOMEC EQUIPMENT, PLEASE CONTACT YOUR USUAL SOCOMEC TECHNICAL CONTACT FOR PERSONALISED HELP IN RESOLVING THE PROBLEM.

ABOUT SOCOMEC

Founded in 1922, SOCOMEC is an independent industrial group with a workforce of 3600 experts spread over 28 subsidiaries in the world. Our core business: the availability, control and safety of low voltage electrical networks serving our customers' power performance. In 2018, SOCOMEC posted a turnover of 537M€.

Revision control

VERSION	DESCRIPTION
Version 1.0 **11 July 2023**	Original Release