SOCOMEC SECURITY NOTIFICATION

SOCOMEC Security Notification

19 November 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 TCP functionality of Socomec DIRIS Digiware M-70 1.6.9. A specially crafted network packet can lead to denial of service and weaken credentials resulting in default documented credentials being applied to the device. An attacker can send an unauthenticated packet to trigger this vulnerability.

Affected Products and Versions

Product Version

Socomec Easy Config System 2.6.1.0 : https://www.socomec.us/en-us/easy-config-system-software

Vulnerability Details

CVE ID: CVE-2024-45370

CVSS v3.1 Base Score 7.3 - CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:C/C:L/I:H/A:N

CWE-302 - Authentication Bypass by Assumed-Immutable Data

The Easy Config System configuration software allows users to configure your Socomec measuring and load-breaking equipment while viewing all the electrical quantities in real-time. It provides features such as auto-detection of connected products and simultaneous configuration of multiple devices. Access to Easy Config System can be done locally by connecting to the products via a USB cable or remotely via the Ethernet network allowing configuration without having to be on site.

The Easy Config System software contains two documented user profiles User and Admin and a third undocumented one called Socomec. The application restricts configuration items available based on the user profile that is currently logged into the application. The application relies on a local sqlite database when presenting a user with the login prompt for the application. This database contains password hashes for each of the user profiles and a field that indicates whether that user is required to enter a password called `passwordActive`. An attacker with system access could modify the database file to disable the requirement to enter a password for any of the user accounts by setting the `passwordActive` field to 0. When this field is 0, the application will not prompt that user for their password before access is granted to the selected user. This would allow the attacker to select the user profile that they wish to access and simply press the login button allowing them access all to all configuration items of connected devices without providing a password to the application.

REMEDIATION

AFFECTED PRODUCT & VERSION	FIX
Previous to Socomec Easy Config System 3.1	New version (3.1) : Easy Config System | Software Socomec

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.

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€.

POWER SWITCHING   POWER MONITORING   POWER CONVERSION   ENERGY STORAGE   EXPERT SERVICES

Revision control

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