SOCOMEC Security Notification

1 October 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 cross-site request forgery (csrf) vulnerability exists in the WEBVIEW-M functionality of Socomec DIRIS Digiware M-70 1.6.9. A specially crafted HTTP request can lead to unauthorized access. An attacker can stage a malicious webpage to trigger this vulnerability.

Affected Products and Versions

Product Version

DIRIS Digiware Webview M-70 1.6.9 Multifunction Communication Gateway DIRIS Digiware M-70 RS485 Ethernet WEBVIEW-M - Reference 48290222

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.

The Socomec M70 webserver, known as WEBVIEW-M utilizes cookies to manage user sessions. The session cookie has the `SameSite` attribute set to `Strict` which instructs the browser that it should not send the cookie in any cross-site requests. Often, this is a sufficient CSRF prevention measure. However, the WEBVIEW-M implementation does not properly handle the scenario where a request is submitted with no session cookie. If a victim visits a malicious web page while logged in to WEBVIEW-M, the browser will behave correctly in that it will not transmit the `sessionid` cookie due to the `SameSite` attribute being set

to `Strict`. When this malicious request is received by the WEBVIEW-M webserver it will be processed as if it was authorized resulting in a successful Cross-site request forgery attack. When the browser sends the malicious request it will be sent within the existing TCP session that has been authenticated. Even though no valid `sessionid` cookie is included in the malicious request, it will be processed and executed by the WEBVIEW-M webserver.

Vulnerability Details

CVE ID: CVE-2024-53684

CVSS v3.1 Base Score 7.5 - CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H

CWE-352 - Cross-Site Request Forgery (CSRF)

A cross-site request forgery (csrf) vulnerability exists in the WEBVIEW-M functionality of Socomec DIRIS Digiware M-70 1.6.9. A specially crafted HTTP request can lead to unauthorized access. An attacker can stage a malicious webpage to trigger this vulnerability.

REMEDIATION

AFFECTED PRODUCT & VERSION	WORKAROUND
Previous to DIRIS Digiware Webview M-50 / M-70 1.7 D-50 / D-70 2.10	New version - D50 https://media.socomec.com/getFileById?fileId=32397128 - D70 https://media.socomec.com/getFileById?fileId=27962768 - M50 https://media.socomec.com/getFileById?fileId=43005259 - M70 - https://media.socomec.com/getFileById?fileId=48881750

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€.