Socomec Security Notification

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.

AFFECTED PRODUCT AND VERSION

PRODUCT

DIRIS A40 ETHERN MODBUS 3I 2O

VERSION

1.8.1

PROBLEM DETAILS

SUBJECT

CVE-2026-2491- DIRIS A-40 HTTP API Authentication Bypass Vulnerability

DESCRIPTION

CVSS : 6.3: AV:A/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L
Trend Micro's Zero Day Initiative has identified a vulnerability affecting the DIRIS A-40

Vulnerability details:
• Product : DIRIS A-40
• Version tested: 1.8.1

Detailled analysis:
The DIRIS-40 power monitoring device is supplied with an Ethernet port, which exposes a web-based interface called WebView for monitoring and configuration of the device. It was discovered that the web interface allows unauthenticated attackers to access all exposed APIs, thus bypassing built-in (client-side) authentication in the web

application. This leads to the attacker gaining an ability to disclose and manipulate device configuration parameters, including stored credentials.

Credit:
Dmitry "InfoSecDJ" Janushkevich of TrendAI Zero Day Initiative

IMPACT

Limited

CVSS	
Attack Vector (AV) Adjacent (A)	**Attack Complexity (AC)** Low (L)
Privileges Required (PR) None (N)	**User Interaction (UI)** None (N)
Scope (S) Unchanged (U)	**Confidentiality (C)** Low (L)
Integrity (I) Low (L)	**Availability (A)** Low (L)
CVSS Score 6,3	**CVSS Criticity** Medium

RESOLUTION INFORMATION

RESOLUTION

To further strengthen the security of the DIRIS A-40 Webview environment, an update will soon be deployed. With this update, the supervision webserver will be disabled by default, and customers will still be able to activate it whenever needed, with a clear information notice to guide them.
This approach ensures a safer default configuration while preserving full flexibility of use.

RECOMMENDATIONS

- For protection, we recommend to install the DIRIS A-40 with Webview on a private network, rather than exposing it directly to public network.
- If Webview is activated, we advise to avoid the use of password-based features, as a precautionary measure.

GENERAL SECURITY RECOMMANDATIONS

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 an incident or a vulnerability? HERE
For further information related to cybersecurity in Socomec's products, visit the company's cybersecurity support portal page HERE.

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.