

SOCOMECS SECURITY NOTIFICATION

SOCOMECS Security Notification

12 January 2024 Document Reference – INT 24 128248

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 lifecycle, Socomec strongly recommend to apply remediations as soon as possible, according your risk assessment.

AFFECTED PRODUCTS AND VERSIONS

Product Version

MODULYS GP (MOD3GP-SY-120K)

Vulnerability Details

CVE ID: CVE-2023-39452

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

A CWE-256: *Plaintext Storage of a Password*

The web application that owns the device clearly stores the credentials within the user management section. Obtaining this information can be done remotely thanks to the incorrect management of the sessions in the web application.

REMEDIATION

AFFECTED PRODUCT & VERSION	REMEDIATION
MODULYS GP (MOD3GP-SY-120K) <i>UPS firmware: Socomec-08BE</i> <i>Web Firmware: 01.12.10</i>	Do not expose product to internet

Socomec recommends to adopt state of the art of cyber security to reduce the risk :

* Not expose product to internet

SOCOMEK SECURITY NOTIFICATION

* Adopt network architectures to minimize exposure (Network segmentation, VLAN, VPN)

* Isolate process products (network diode, sealed solution, ...)

* Use adequate protection to prevent intrusions (applicative firewall, bastion, IPS, ...)

In this manner, the product will be isolated and its potential attack surface reduced, reducing the likelihood.

In addition, for information, this product has been replaced by MODULYS GP2 (M4-S-XXX) in 2014, native secured, and attested from a certified third party. This current version is regularly updated to protect it against new vulnerabilities.

SOCOMEK SECURITY NOTIFICATION

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 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](#).

LEGAL DISCLAIMER

SOCOMEK SECURITY NOTIFICATIONS AND ALL THE INFORMATION CONTAINED THEREIN ARE INTENDED TO INFORM ANY USER OF EQUIPMENT MARKETED BY THE SOCOMEK GROUP (“SOCOMEK”) 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

SOCOMEK SECURITY NOTIFICATION

SITUATION AND WITHOUT ANY GUARANTEE WHATSOEVER, IN PARTICULAR AS TO ITS SUITABILITY FOR ANY PROBLEMS ENCOUNTERED BY THE USER.

IN NO EVENT SHALL SOCOMEK 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 SOCOMEK 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.

SOCOMEK 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 SOCOMEK EQUIPMENT, PLEASE CONTACT YOUR USUAL SOCOMEK TECHNICAL CONTACT FOR PERSONALISED HELP IN RESOLVING THE PROBLEM.

ABOUT SOCOMEK

Founded in 1922, SOCOMEK 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, SOCOMEK posted a turnover of 537M€.



POWER
SWITCHING



POWER
MONITORING



POWER
CONVERSION



ENERGY
STORAGE



EXPERT
SERVICES

Revision control

VERSION

Version 1.0
11 July 2023

DESCRIPTION

Original Release