DOCUMENT ID: 2NGA002356
REVISION: A
DATE: 2024-09-10

CYBER SECURITY ADVISORY

ABB Relion 630 Series Protection Relays IEC 61850 MMS and improper Input Validation Vulnerabilities

CVE ID: CVE-2022-3353, CVE-2023-4518

Notice

The information in this document is subject to change without notice, and should not be construed as a commitment by ABB.

ABB provides no warranty, express or implied, including warranties of merchantability and fitness for a particular purpose, for the information contained in this document, and assumes no responsibility for any errors that may appear in this document. In no event shall ABB or any of its suppliers be liable for direct, indirect, special, incidental or consequential damages of any nature or kind arising from the use of this document, or from the use of any hardware or software described in this document, even if ABB or its suppliers have been advised of the possibility of such damages.

This document and parts hereof must not be reproduced or copied without written permission from ABB, and the contents hereof must not be imparted to a third party nor used for any unauthorized purpose.

All rights to registrations and trademarks reside with their respective owners.

© Copyright 2024 ABB. All rights reserved.

Purpose

ABB has a rigorous internal cyber security continuous improvement process which involves regular testing with industry leading tools and periodic assessments to identify potential product issues. Occasionally an issue is determined to be a design or coding flaw with implications that may impact product cyber security.

When a potential product vulnerability is identified or reported, ABB immediately initiates our vulnerability handling process. This entails validating if the issue is in fact a product issue, identifying root causes, determining what related products may be impacted, developing a remediation, and notifying end users and governmental organizations.

The resulting Cyber Security Advisory intends to notify customers of the vulnerability and provide details on which products are impacted, how to mitigate the vulnerability or explain workarounds that minimize the potential risk as much as possible. The release of a Cyber Security Advisory should not be misconstrued as an affirmation or indication of an active threat or ongoing campaign targeting the products mentioned here. If ABB is aware of any specific threats, it will be clearly mentioned in the communication.

The publication of this Cyber Security Advisory is an example of ABB's commitment to the user community in support of this critical topic. Responsible disclosure is an important element in the chain of trust we work to maintain with our many customers. The release of an Advisory provides timely information which is essential to help ensure our customers are fully informed.

Affected products

The following products are affected: REF630, REG630, REM630 and RET630.
The affected firmware versions are as follows:

- 1.1.0.C4 or earlier for 630 series 1.1
- 1.2.0.B7 or earlier for 630 series 1.2
- 1.3.0.B0 or earlier for 630 series 1.3

Vulnerability IDs

CVE-2022-3353, CVE-2023-4518

ABBVREP0128

Summary

An update is available that resolves publicly reported vulnerabilities in the product versions listed above.

CVE-2022-3353

An attacker who successfully exploited this vulnerability could cause the product to stop accepting new IEC 61850 MMS client connections.

CVE-2023-4518

An attacker who successfully exploited this vulnerability could cause the product to restart.

© Copyright 2024 ABB. All rights reserved.

Recommended immediate actions

The problem is corrected in the following firmware versions:

- 1.1.0.C5 for 630 series 1.1
- 1.2.0.B8 for 630 series 1.2
- 1.3.0.B1 for 630 series 1.3

ABB recommends that customers apply the update at earliest convenience. Refer to the following link: https://relays.protection-control.abb/downloads/firmware-updates

Vulnerability severity and details

The severity assessment has been performed by using the FIRST Common Vulnerability Scoring System (CVSS) for both v3.1[1] and v4.0[2].

CVE-2022-3353
An attacker could exploit the vulnerability by using a specially crafted message sequence to force the IEC 61850 MMS-server communication stack to stop accepting new MMS-client connections. Already existing/established client-server connections are not affected.

CVSS v3.1 Base Score: 5.9
CVSS v3.1 Temporal Score: 5.3
CVSS v3.1 Vector: AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C
CVSS v4.0 Score: 8.2
CVSS v4.0 Vector:
CVSS:4.0/AV:N/AC:H/AT:N/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N/S:P/AU:N/R:U/V:D/RE:M/U:Amber
NVD Summary Link: https://nvd.nist.gov/vuln/detail/CVE-2022-3353

CVE-2023-4518
A vulnerability exists in the input validation of the GOOSE messages, where out of range values received and processed by the IED caused a reboot of the device. For an attacker to exploit the vulnerability, GOOSE receiving blocks need to be configured.

CVSS v3.1 Base Score: 6.5
CVSS v3.1 Temporal Score: 5.9
CVSS v3.1 Vector: AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C
CVSS v4.0 Score: 7.1
CVSS v4.0 Vector:
CVSS:4.0/AV:A/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N/S:P/AU:N/R:A/V:D/RE:M/U:Amber
NVD Summary Link: https://nvd.nist.gov/vuln/detail/CVE-2023-4518

[1] For the CVSS v3.1 scoring only the CVSS Base Score and the Temporal Score (if information is available) are considered in this advisory. The CVSS Environmental Score, which can affect the vulnerability severity, is not provided in this advisory since it reflects the potential impact of a vulnerability within the end-user organizations' computing environment; end-user organizations are therefore recommended to analyze their situation and specify the Environmental Score.

[2] For the CVSS v4.0 scoring only the CVSS Base Metrics and the CVSS Supplemental Metrics (if information is available) are considered in this advisory. The CVSS Environmental and Threat Metrics, which can affect the vulnerability severity, are not provided in this advisory since they reflect the potential impact of a vulnerability within the end-user organizations' computing environment and over time depending on the vulnerability exploit maturity. Therefore, end-user organizations are recommended to analyze their situation and specify the Environmental and Threat Metrics.

© Copyright 2024 ABB. All rights reserved.

Mitigating factors

Refer to section “General security recommendations” for further advise on how to keep your system secure.

Frequently asked questions

What causes the vulnerability CVE-2022-3353?

The vulnerability is caused by a flaw in the MMS server's communication stack, which stops accepting new MMS client connections when a specially crafted message sequence was sent to the stack.

What causes the vulnerability CVE-2023-4518?

The vulnerability is caused by a flaw in the input validation of GOOSE messages, which allows out of range values to be processed by the device.

What is ABB Relion 630?

The ABB Relion 630 series is a family of protection and control relays designed for power distribution networks and industrial applications. These relays offer flexible and scalable functionality to meet various customer needs, including feeder, transformer, and motor protection and control.

What is IEC 61850 MMS?

MMS (Manufacturing Message Specification) is a communication protocol defined within the IEC 61850 standard, which is used for communication in electrical substations. MMS is a client/server-based protocol that facilitates the exchange of information between Intelligent Electronic Devices, such as protection relays, and higher-level systems like SCADA (Supervisory Control and Data Acquisition) over Ethernet networks.

What is IEC 61850 GOOSE?

GOOSE (Generic Object-Oriented Substation Event) is a communication protocol defined by the IEC 61850 standard. GOOSE is a publisher-subscriber-based protocol, used in electrical substations for fast and reliable data exchange between Intelligent Electronic Devices, such as protection relays, over Ethernet networks.

What is input validation?

Input validation is a security measure that ensures data entering a system is correct. It involves checking that inputs from users or external systems meet specific criteria before being processed by the application.

What might an attacker use the vulnerability to do?

CVE-2022-3353

The attacker could cause a denial-of-service type of situation, where the device stops accepting new MMS client connections.

CVE-2023-4518

The attacker could force the device to reboot, causing operational disruption of the device.

© Copyright 2024 ABB. All rights reserved.

How could an attacker exploit the vulnerability?

CVE-2022-3353

The attacker who successfully exploited this vulnerability could send a specially crafted message sequence to the device, causing it to stop accepting new MMS client connections. A manual reboot would be needed to restore the device's capability of accepting new MMS client connections.

This would require that the attacker has access to the system network, by connecting to the network either directly or through a wrongly configured or penetrated firewall, or that they install malicious software on a system node or otherwise infects the network with malicious software. Recommended practices help mitigate such attacks, see section Mitigating Factors above.

CVE-2023-4518

The attacker who successfully exploited this vulnerability could send a GOOSE message with values out of range to the device, causing it to reboot. During reboot, there is an operational disruption of the device.

This would require that the attacker has access to the system network, by connecting to the network either directly or through a wrongly configured or penetrated firewall, or that they install malicious software on a system node or otherwise infects the network with malicious software. Recommended practices help mitigate such attacks, see section Mitigating Factors above.

Could these vulnerabilities be exploited remotely?

Yes, an attacker who has network access to an affected system node could exploit this vulnerability.

Recommended practices include that process control systems are physically protected, have no direct connections to the Internet, and are separated from other networks by means of a firewall system that has a minimal number of ports exposed.

Can functional safety be affected by exploiting these vulnerabilities?

Yes, provided that the attacker has access to the system network. Denial-of-service or device reboot may have safety implications.

What does the update do?

CVE-2022-3353

The update removes the vulnerability by changing the behavior of the IEC 61850 MMS communication.

CVE-2023-4518

The update removes the vulnerability by modifying the way that the device validates values in the GOOSE messages.

When this security advisory was issued, had these vulnerabilities been publicly disclosed?

Yes, these vulnerabilities have been publicly disclosed.

When this security advisory was issued, had ABB received any reports that these vulnerabilities were being exploited?

No, ABB had not received any information indicating that these vulnerabilities had been exploited when this security advisory was originally issued.

© Copyright 2024 ABB. All rights reserved.

General security recommendations

For any installation of software-related ABB products we strongly recommend the following (non-exhaustive) list of cyber security practices:

- Isolate special purpose networks (e.g. for automation systems) and remote devices behind firewalls and separate them from any general-purpose network (e.g. office or home networks).
- Install physical controls so no unauthorized personnel can access your devices, components, peripheral equipment, and networks.
- Never connect programming software or computers containing programing software to any network other than the network for the devices that it is intended for.
- Scan all data imported into your environment before use to detect potential malware infections.
- Minimize network exposure for all applications and endpoints to ensure that they are not accessible from the Internet unless they are designed for such exposure and the intended use requires such.
- Ensure all nodes are always up to date in terms of installed software, operating system, and firmware patches as well as anti-virus and firewall.
- 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.

References

1MRS756793, Rev. E	630 series IEC 61850 Communication Protocol Manual

Support

For additional instructions and support please contact your local ABB service organization. For contact information, see www.abb.com/contactcenters.

Information about ABB's cyber security program and capabilities can be found at www.abb.com/cybersecurity.

Revision history

Rev. Ind.	Page (p) Chapter (c)	Change description	Rev. date
A	all	Initial version	Sep-10-2024

© Copyright 2024 ABB. All rights reserved.