DOCUMENT ID: 2NGA001911
REVISION: A
DATE: 2024-10-21

CYBER SECURITY ADVISORY

ABB Relion 611, 615, 620, 630 series, REX610, REX640, SMU615, SSC600, Arctic solution, COM600, SPA ZC-400, SUE3000 Guidelines to Prevent Unauthorized Modifications of Firmware and Configuration

CVE ID: CVE-2024-8036

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.

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

ABB Relion Protection Relays 611, 615, 620 and 630 series, REC/RER615/620, REX610, REX615 and REX640

ABB Substation Merging Unit SMU615

ABB Smart Substation Control and Protection SSC600

ABB communication solution products ARG/ARC/ARR/ARP600, RER/REC601/603, ARM600, and ARM600SW

ABB digital substation products COM600, SPA ZC-400/402

SUE3000

Vulnerability ID

CVE-2024-8036

Summary

ABB is aware of privately reported vulnerability in the product versions listed above.

An attacker who successfully exploited this vulnerability could manipulate the firmware and configuration of the product.

Recommended immediate actions

ABB recommends that customers follow the measures described in the released Product Advisory note in the following link Guidelines to Prevent Unauthorized Modifications of Firmware and Configuration, ABB Digital Substation Products at earliest convenience.

Vulnerability severity and details

A vulnerability exists in the firmware and configuration update included in the product versions listed above. An attacker could exploit the vulnerability by sending a specially crafted firmware or configuration to the system node, causing the node to stop, or become inaccessible, or allowing the attacker to take control of the node.

The severity assessment has been performed by using the FIRST Common Vulnerability Scoring System (CVSS) v3.1[1].

CVE-2024-8036

The product does not itself check the authenticity and integrity of the firmware or configuration but relies on the engineering tool's verification.

CVSS v3.1 Base Score:	5.9
CVSS v3.1 Temporal Score:	5.4
CVSS v3.1 Vector:	AV:A/AC:H/PR:H/UI:R/S:U/C:L/I:H/A:H/E:P/RL:W/RC:C
CVSS v4.0 Score:	4.6
CVSS v4.0 Vector:	CVSS:4.0/AV:A/AC:H/AT:P/PR:H/UI:P/VC:L/VI:H/VA:H/SC:N/SI:N/SA:N/S:P/AU:N/R:I/V:D/RE:H/U:Amber
Summary Link:	https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-8036

Mitigating factors

Please follow the guidelines in the following Product Advisory Note to improve the system security:

Guidelines to Prevent Unauthorized Modifications of Firmware and Configuration, ABB Digital Substation Products

[1] 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.

Frequently asked questions

What is the scope of the vulnerability?

An attacker who successfully exploited this vulnerability could manipulate the firmware and configuration of the product.

What causes the vulnerability?

The checking of the digital signature of the firmware update package is done by Protection and Control Manager tool PCM600. The affected devices are not checking the digital signature of the firmware or configuration. If the attacker could find out the administrator or other privileged user's password, they could be able to update the product’s firmware or configuration to malicious one, causing unpredictable behavior.

What might an attacker use the vulnerability to do?

An attacker who successfully exploited this vulnerability could cause the product to stop, make the product inaccessible, or take control of the product.

How could an attacker exploit the vulnerability?

The following preconditions must be met.

- The attacker must be able to gain access to the substation network by using undefined attack method, e.g., locally or through a wrongly configured or penetrated firewall.
- The attacker must be able to find out the administrator/engineer user's password, e.g., unchanged factory default password or password captured from non-encrypted traffic.

If these preconditions are met, the attacker could be able to update the device’s firmware by transferring the firmware update binary files to the device or to change the device’s configuration.

Could the vulnerability be exploited remotely?

Yes, an attacker who has access to the substation network could exploit this vulnerability. Recommended practices include that electrical substations 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 and protocols exposed.

Can functional safety be affected by an exploit of this vulnerability?

Yes, if the attacker can render the device inoperable or take control of the device.

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

No, the vulnerability has not been publicly disclosed.

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

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

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.
- 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.

Acknowledgement

ABB thanks Jos Wetzels from Midnight Blue (midnightblue.nl) for helping to identify the vulnerabilities and protecting our customers.

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	Oct-21-2024