ABB Doc Id: 2NGA000934
REVISION: -
DATE: 2021-03-12

CYBER SECURITY ADVISORY

Denial of Service Vulnerability in ABB Relion 630 Series 61850 communication

ABBVU-ABBVREP0041-ELDS2110

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.

Affected Products

The products listed in the table are affected by the vulnerability.

Product / System line	Products and Affected Versions	Advisory
Relion 630 series	REF630, REM630, RET630, REG630 protection relays with firmware versions prior to • 1.3.0.A9 for 630 series 1.3 • 1.2.0.B6 for 630 series 1.2 • 1.1.0.C3 for 630 series 1.1	Advisory

ABB products not listed are initially evaluated as not impacted. ABB continues to evaluate the vulnerabilities and will update the advisory when additional information becomes available

Vulnerability ID

ABB ID: ABBVU-ABBVREP0041-ELDS2110
CVE ID: CVE-2021-27196

Summary

A privately reported vulnerability in which an attacker having access to the IEC 61850 network with knowledge on how to reproduce the attack and knowing the IP addresses of the IEC 61850 access points of the IEDs can reproduce this attack and force the IEDs to reboot, resulting in a denial of service situation. During this time, the primary functionality of the device is not available.

Vulnerability Severity

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

CVSS v3.1 Base Score: 7.5

CVSS v3.1 Temporal Score: 7.2

CVSS v3.1 Vector: AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:H/RL:O/RC:C

CVSS v3.1 Link:

https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?vector=AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:H/RL:O/RC:C&version=3.1

Vulnerability Details

A vulnerability exists in the command handling of the IEC 61850 communication stack included in the product revisions listed above. An attacker could exploit the vulnerability by using a specially crafted 61850 message and force the device to reboot.

Mitigating Factors

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.
In general protection, control & automation systems should not be used for general business functions which are not critical industrial processes. Portable computers and removable storage media should be carefully scanned for viruses before they are connected to a control system. Block all non-trusted IP communications.

Advisory for Relion® 630 series

Please update the Relion® 630 series IEC firmware:

- Firmware update release 1.3.0.A9 for 630 series 1.3
- Firmware update release 1.2.0.B6 for 630 series 1.2
- Firmware update release 1.1.0.C3 for 630 series 1.1

The firmware updates can be downloaded from https://protection.datacare.abb.com/

Frequently Asked Questions

What is the scope of the vulnerability?

An attacker having access to the IEC 61850 network can force the IEDs to reboot by sending a specially crafted message sequence. This will result in a denial of service including the primary functionality of the device.

What causes the vulnerability?

The vulnerability is caused by a weakness in the message processing in the IEC 61850 protocol.

How could an attacker exploit the vulnerability?

An attacker could try to exploit the vulnerability by creating a specially crafted message and sending the message to an affected system node. 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 he installs malicious software on a system node or otherwise infects the network with malicious software.

Could the vulnerability be exploited remotely?

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

Do the advisories mitigate the issue?

Yes, following the advisories mitigates the identified weakness in the IEC 61850 protocol handling.

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

No.

Acknowledgements

ABB thanks Markus Mahrla, GAI NetConsult GmbH and Lars Lengersdorf, Amprion GmbH for helping to identify the vulnerability and protecting our customers

Support

For additional information and support please contact your product provider or ABB service organization. For contact information, see https://new.abb.com/contact-centers Information about ABB's cyber security program and capabilities can be found at https://www.abb.com/cybersecurity.