ABB DOC ID: 1MRG027165
REVISION: A
DATE: 2019-10-22

CYBER SECURITY ADVISORY

Terminal Reboot Vulnerability in Relion® 650 series and Relion® 670 series

ABBVU-PGGA-1MRG027165

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.

Affected Products

Relion 650 1.3.0.5 and previous releases

Relion 670 1.2.3.18 and previous releases

Relion 670 2.0.0.11 and previous releases

Relion 670 2.1.0.1 and previous releases

Vulnerability ID

ABB ID: ABBVU-PGGA-1MRG027165

Summary

A privately reported vulnerability in command handling on SPA protocol over TCP/IP is available in the product versions listed above.

An attacker who successfully exploited this vulnerability could reboot the device resulting in a denial of service situation. During the reboot phase, the primary functionality of the device is not available.

The vulnerability is related to test command that is not documented. The reboot operation could also be triggered by sending the documented SPA code to the device through a SPA client.

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 Base Score: 5.3 (Medium)

CVSS v3 Temporal Score: 4.8 (Medium)

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

CVSS v3 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:L/E:P/RL:O/RC:C

Recommended immediate actions

The problem is corrected in the following product versions:

- Relion 650 1.3.0.6
- Relion 670 1.2.3.19
- Relion 670 2.0.0.12
- Relion 670 2.1.0.2

ABB recommends that customers apply the update at the earliest convenience.

Vulnerability Details

A vulnerability exists in the command handling of the device included in the product versions listed above. An attacker could exploit the vulnerability by using a specially crafted message and force the device to reboot. During reboot, the primary protection functionality is not available.

The vulnerability is related to test command that is not documented. The reboot operation could also be triggered by sending the documented SPA code to the device througt an SPA client.

Mitigating Factors

Recommended security practices and firewall configurations can help protect a process control network from attacks that originate from outside the network. Such practices include that process control systems are physically protected from direct access by unauthorized personnel, 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, and others that have to be evaluated case by case. Process control systems should not be used for Internet surfing, instant messaging, or receiving e-mails. Portable computers and removable storage media should be carefully scanned for viruses before they are connected to a control system.

More information on recommended practices can be found in the Cyber Security Deployment Guidelines for each product version.

Workarounds

ABB has not identified any workaround; however, firewall rules could be set to block incoming traffic to port 7001/TCP that originate from outside the network.

In the Relion® 650 series version 1.3, the SPA protocol over TCP/IP could be disabled if it is not in use.

Frequently Asked Questions

What is the scope of the vulnerability?

An attacker who successfully exploited this vulnerability could reboot the device resulting in a denial of service situation. During the reboot phase, the primary functionality of the device is not available.

What causes the vulnerability?

The vulnerability is caused by the releasing of test commands in the SPA protocol implementation.

What might an attacker use the vulnerability to do?

An attacker who successfully exploited this vulnerability could reboot the device resulting in a denial of service situation. During the reboot phase, the primary functionality of the device is not available.

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. Recommended practices help mitigate such attacks, see section Mitigating Factors above.

Could the vulnerability 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.

What does the update do?

The update removes the test commands from product code.

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

No, ABB received information about this vulnerability through responsible disclosure.

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.

Acknowledgements

ABB thanks the following individuals from an independent group, ScadaX, for working with us to help protect customers:

- Ilya Karpov (ScadaX)
- Evgeniy Druzhinin (ScadaX)
- Victor Nikitin (ScadaX).

Support

For additional information and support please contact your local 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 www.abb.com/cybersecurity.