ABB DOC ID: 1MRG032388
REVISION: A
DATE: 2019-10-22

CYBER SECURITY ADVISORY

# OpenSSL vulnerabilities in Relion® 670 series and Relion® 650 series

## ABBVU-PGGA-1MRG032388

## 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 series version 1.3.0.0 to version 1.3.0.5.
- Relion 650 series version 2.1.0.0 to version 2.1.0.2.
- Relion 670 series version 2.1.0.0 to version 2.1.0.2.

# Vulnerability ID

ABB ID: ABBVU-PGGA-1MRG032388

CVE ID: CVE-2017-3737, CVE-2018-0739, CVE-2018-0737, CVE-2018-0732

# Summary

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

An attacker who successfully exploited these vulnerabilities could have access to sensitive information or cause a Denial Of service of the affected IEDs.

# 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.

CVE-2017-3737

CVSS v3 Base Score: 5.9 (Medium)

CVSS v3 Temporal Score: 5.5

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

CVSS v3 Link https://nvd.nist.gov/vuln/detail/CVE-2017-3737

CVE-2018-0739

CVSS v3 Base Score: 6.5 (Medium)

CVSS v3 Temporal Score: 5.9

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

CVSS v3 Link https://nvd.nist.gov/vuln/detail/CVE-2018-0739

CVE-2018-0737

CVSS v3 Base Score: 5.9 (Medium)

CVSS v3 Temporal Score: 5.5

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

| | |
|---|---|
| CVSS v3 Link | https://nvd.nist.gov/vuln/detail/CVE-2018-0737 |

CVE-2018-0732

| | |
|---|---|
| CVSS v3 Base Score: | 7.5 (High) |
| CVSS v3 Temporal Score: | 7.0 |
| CVSS v3 Vector: | AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:F/RL:O/RC:C |
| CVSS v3 Link | https://nvd.nist.gov/vuln/detail/CVE-2018-0732 |

## Recommended immediate actions

The problem is corrected in:

- Relion 650 series version 1.3.0.6
- Relion 650 series version 2.1.0.3
- Relion 670 series version 2.1.0.3

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

## Vulnerability Details

CVE-2017-3737

The error mechanism implemented in OpenSSL that prevents the application to continue with a failed handshake has issues when called certain functions are called instead of explicit handshake functions.

CVE-2018-0739

Constructed ASN.1 types with a recursive definition could eventually exceed the stack given malicious input with excessive recursion which

CVE-2018-0737

The openSSL RSA Key generation algorithm has been shown to be vulnerable to a cache timing side channel attack.

CVE-2018-0732

During key agreement in a TLS handshake using a DH(E) based ciphersuite, a malicious server can send a very large prime value to the client which it will spend an unreasonable long period of time generating a key for this prime.

## 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.

Industrial 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.

# Workarounds

No workarounds have been identified by the vendor.

# Frequently Asked Questions

## What causes the vulnerability?

These vulnerabilities are caused by weaknesses in the OpenSSL library used by the product.

## What might an attacker use the vulnerability to do?

An attacker who successfully exploited these vulnerabilities could cause a DoS of affected IED by processing constructed data or allow a compromise of data confidentiality by transmitting it unencrypted over the network.

## How could an attacker exploit the vulnerability?

An attacker could try to exploit this vulnerabilities by creating specially crafted message and sending it an affected IED. 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 vulnerability by using a version of OpenSSL library where the vulnerabilities are fixed.

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

Yes, this vulnerability has been publicly disclosed.

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

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

# 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.