ABB DOC ID: 1MRG025160
REVISION: A
DATE: 2019-10-22

CYBER SECURITY ADVISORY

OpenSSL vulnerabilities in Relion® 650 series version 2.1 and Relion® 670 series version 2.1

ABB-VU-PGGA-1MRG024369
ABB-VU-PGGA-1MRG025160

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

Relion 650 series version 2.1.0.2 and previous releases.

Relion 670 series version 2.1.0.2 and previous releases.

Vulnerability ID

ABB ID: ABB-VU-PGGA-1MRG024369

CVE ID: CVE-2016-2109

ABB ID: ABB-VU-PGGA-1MRG025160

CVE ID: CVE-2016-2177, CVE-2016-2178, CVE-2016-2182, CVE-2016-2183, CVE-2016-6304, CVE-2016-6306

Summary

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

An attacker who successfully exploited this vulnerability could cause a DoS of affected IED by allocating large amounts of memory potentially consuming excessive resources or exhausting memory.

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-2016-2109

CVSS v3 Base Score:	7.5 (High)
CVSS v3 Temporal Score:	6.7
CVSS v3 Vector:	AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C
CVSS v3 Link	https://nvd.nist.gov/vuln/detail/CVE-2016-2109

CVE-2016-2177

CVSS v3 Base Score:	9.8 (Critical)
CVSS v3 Temporal Score:	8.8
CVSS v3 Vector:	AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CVSS v3 Link	https://nvd.nist.gov/vuln/detail/CVE-2016-2177

CVE-2016-2178

CVSS v3 Base Score:	5.5 (Medium)
CVSS v3 Temporal Score:	5.1
CVSS v3 Vector:	AV:L/AC:L/PR:L/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-2016-2178

CVE-2016-2182

CVSS v3 Base Score:	9.8 (Critical)
CVSS v3 Temporal Score:	8.5
CVSS v3 Vector:	AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C
CVSS v3 Link	https://nvd.nist.gov/vuln/detail/CVE-2016-2182

CVE-2016-2183

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:H/I:N/A:N/E:F/RL:O/RC:C
CVSS v3 Link	https://nvd.nist.gov/vuln/detail/CVE-2016-2183

CVE-2016-6304

CVSS v3 Base Score:	7.5 (High)
CVSS v3 Temporal Score:	6.7
CVSS v3 Vector:	AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C
CVSS v3 Link	https://nvd.nist.gov/vuln/detail/CVE-2016-6304

CVE-2016-6306

CVSS v3 Base Score:	5.9 (Medium)
CVSS v3 Temporal Score:	5.2
CVSS v3 Vector:	AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H/E:U/RL:O/RC:C
CVSS v3 Link	https://nvd.nist.gov/vuln/detail/CVE-2016-6306

Recommended immediate actions

The problem is corrected in the following product versions:

Relion 650 series version 2.1.0.3 and Relion 670 series version 2.1.0.3.

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

Vulnerability Details

CVE-2016-2109

Parsing ASN.1 untrusted data can cause allocation of large amounts of memory potentially consuming excessive resources or exhausting.

CVE-2016-2177

Multiple integer overflow flaws were found in the way OpenSSL library performed pointer arithmetic.

CVE-2016-2178

When DSA certificates has been deployed in the IED (rare since the official tool generates RSA certificates) an attacker could discover the DSA private key via a timing side-channel attack.

CVE-2016-2182

Improperly validation of division results could result in a denial of service through out-of-bound writes.

CVE-2016-2183

Triple-DES cipher, as used in the TLS protocol could be used to obtain clear text data via a birthday attack against a long-duration encrypted sessions.

CVE-2016-6304

Excessively large OCSP Status Request sent to the device continually will lead a denial of service attack through memory exhaustion.

CVE-2016-6306

Parsing crafted certificates will lead to a denial of service through out-of-bound read.

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 vulnerabilities?

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

What is the affected component?

The following products are affected:

Relion 650 series version 2.1.0.2 and previous releases.

Relion 670 series version 2.1.0.2 and previous releases.

What might an attacker use the vulnerability to do?

An attacker who successfully exploited this vulnerability could cause a DoS of affected IED by allocating large amounts of memory potentially consuming excessive resources or exhausting memory.

How could an attacker exploit the vulnerability?

See impact in section “Vulnerability Details” above.

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 vulnerabilities by using a version of the OpenSSL library where the vulnerability is 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 and www.abb.com/protection-control

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