MMS Path Traversal Vulnerability in Relion® 670 series

ABB-VU-PPGA-1MRG024910

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 670 series version 1p1r26 and earlier releases
Relion 670 series version 1.2.3.17 and earlier releases
Relion 670 series version 2.0.0.10 and earlier releases (RES670 2.0.0.4 and earlier releases)
Relion 670 series version 2.1.0.1 and earlier releases

Vulnerability ID

ABB ID: ABB-VU-PPGA-1MRG024910

Summary

An update is available that resolves a privately reported vulnerability in IEC 61850 MMS service running in the product versions listed above.

An attacker who successfully exploited this vulnerability could retrieve any file on the device’s flash drive without authentication on the device or make the product inoperative by deleting files from the device’s flash drive.

Vulnerability Severity

The severity assessment has been performed by using the FIRST Common Vulnerability Scoring System (CVSS) for both CVSS v2 and 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 v2 Base Score:	10 (High)
CVSS v2 Temporal Score:	8,3 (High)
CVSS v2 Vector:	AV:N/AC:L/Au:N/C:C/I:C/A:C/E:F/RL:OF/RC:C

CVSS v2 Link:
http://nvd.nist.gov/cvss.cfm?version=2&vector=(AV:N/AC:L/Au:N/C:C/I:C/A:C/E:F/RL:OF/RC:C)

CVSS v3 Base Score:	10 (Critical)
CVSS v3 Temporal Score:	9,3 (Critical)
CVSS v3 Vector:	AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H/E:F/RL:O/RC:C

CVSS v3 Link:

http://nvd.nist.gov/cvss/v3-calculator?vector=AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H/E:F/RL:O/RC:C

Corrective Action or Resolution

The problem is corrected in the following product versions:

- Relion 670 series version 1p1r27
- Relion 670 series version 1.2.3.18
- Relion 670 series version 2.0.0.11 (RES670 2.0.0.5)
- Relion 670 series version 2.1.0.2

ABB recommends that customers apply the update at earliest convenience if IEC 61850 is used.

Vulnerability Details

A vulnerability exists in the MMS server included in the product versions listed above. An attacker could exploit the vulnerability by using specially crafted paths in the *fopen* or *fdelete* requests to read/delete files outside the COMTRADE directory.

Mitigating Factors

Recommended security practices and firewall configurations (including VPN) 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/services 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.

If IEC 61850 protocol isn't used, make sure it is disabled. This removes the vulnerability.

Workarounds

The only known workaround is to disable IEC 61850 protocol when it isn't used. If this is not the case, ABB recommends having a proper security architecture that divides the system in different security zones and revise the firewall configurations to limit the usage of MMS protocol to the relevant upper networks.

IEC 61850 MMS protocol uses TCP port 102.

Frequently asked questions

What is the scope of the vulnerability?

An attacker who successfully exploited this vulnerability could retrieve any file on the device's flash drive without authentication on the device or make the product inoperative by deleting files from the device's flash drive.

What causes the vulnerability?
The vulnerability is caused by unchecked input data in the IEC 61850 MMS server in the 670 series.

What is the IEC 61850 MMS server?
The MMS (Manufacturing Message Specification) is part of the IEC 61850 protocol and it is used for transferring real time process data and supervisory control information between devices.

What might an attacker use the vulnerability to do?
An attacker who successfully exploited this vulnerability could retrieve any file on the device's flash drive without authentication on the device or make the product inoperative by deleting files from the device's flash drive.

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 device. 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/services exposed.

What does the update do?
The update removes the vulnerability by modifying the way that the MMS server verify input data for paths in the requests.

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 for working with us to help protect customers:

- Kirill Nesterov (Kaspersky Lab) for discovering this vulnerability.

Support

For additional information and support please contact your local ABB service organization. For contact information, see www.abb.com.

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