DOCUMENT ID: 2NGA001147
REVISION: A
DATE: 2021-11-29

CYBERSECURITY ADVISORY

MMS File Transfer Vulnerability impact on Distribution Automation products

CVE ID: CVE-2021-22283

ABBVREP0060-ELDS2147

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

Product type	Products and Affected Versions
Protection and Control Relays	611 series: All existing firmware versions. REF615 IEC 1.0: All existing firmware versions REF615 ANSI 1.0: All existing firmware versions REF615 IEC 1.1: All existing firmware versions RED615 IEC 1.1: All existing firmware versions REF615 ANSI 1.1: All existing firmware versions 615 series IEC 2.0: All existing firmware versions 615 series CN 2.0: All existing firmware versions 615 series ANSI 2.0: All existing firmware versions 615 series 3.1 CN: All existing firmware versions 615 series IEC 3.0: All existing firmware versions 615 series CN 3.0: All existing firmware versions 615 series IEC 4.0: All existing firmware versions 615 series ANSI 4.0: All existing firmware versions 615 series IEC 4.0 FP1: All existing firmware versions 615 series CN 4.0 FP1: All existing firmware versions 615 series ANSI 4.0 FP1: All existing firmware versions 615 series ANSI 4.0 FP2: All existing firmware versions 615 series IEC 5.0: All existing firmware versions 615 series IEC 5.0 FP1: All existing firmware versions 615 series CN 5.0 FP1: All existing firmware versions 615 series ANSI 5.0 FP1: All existing firmware versions RER620: All existing firmware versions 620 series IEC/CN 2.0: All existing firmware versions 620 series IEC/CN 2.0 FP1: All existing firmware versions 620 series ANSI: All existing firmware versions REX640 PCL1: All existing firmware versions REX640 PCL2: All existing firmware versions REF615R: All existing firmware versions

Product type	Products and Affected Versions
	RER615: All existing firmware versions
Circuit-Breaker with Integrated Protection	eVD4 equipped with RBX615: All existing firmware versions
Remote Monitoring and Control	REC615: All existing firmware versions
Merging Unit	SMU615: All existing firmware versions

Vulnerability ID

ABBID: ABBVREP0060

Summary

During substation on-site testing, it was noticed that disturbance records could not be retrieved from the device after few successful retrieval attempts. Device detected error in file system with internal fault indication code 7.

ABB has analyzed the problem which was caused when MMS clients attempted to open multiple files without closing them. This eventually blocked also other protocols and internal file handling to have access to the file system due to an internal defense mechanism which prevents file access when the open file handle limit is met.

The products listed in this document are affected by the vulnerability described in this document. Firmware updates will be announced at a later stage and this advisory will be updated accordingly.

Vulnerability severity

The severity assessment has been performed by using the FIRST Common Vulnerability Scoring System (CVSS) v3.1.

CVSS v3.1 Base Score:	6.2
CVSS v3.1 Temporal Score:	5.9
CVSS v3.1 Overall Score	7.6
CVSS v3.1 Vector:	AV:L/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:F/RL:W/RC:C
CVSS v3.1 Link:	https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:F/RL:W/RC:C

Recommended actions

To minimize the risk of the MMS file transfer vulnerabilities users should take these defensive measures:

- Avoid exposure of the devices to the Internet and use secure methods like VPN when accessing them remotely.
- Locate the control system network behind a firewall and segregate them from other networks.
- Use File transfer protocol for reading disturbance records.
- If MMS file transfer must be used as a proxy service for remote connections, use always latest MMS file transfer client software version.
- REX640: Disable MMS access for ports which are not used to access the relay using MMS protocol.

Vulnerability details

The products listed in this advisory have vulnerability. An attacker could exploit the vulnerabilities by using specially crafted MMS client which opens multiple files with file open request without never closing the files. This would cause the relay to go to internal fault state.

Frequently asked questions

What is the scope of the vulnerability?

An attacker who successfully exploited this vulnerability could block the communication to the SCADA system and set the relay to internal fault state.

What causes the vulnerability?

The vulnerability is caused by a flaw in the file system integrated into the devices.

What might an attacker use the vulnerability to do?

An attacker who successfully exploited this vulnerability could cause the communication to the SCADA system to stop or become inaccessible and set relay to internal fault state.

How could an attacker exploit the vulnerability?

An attacker must use specially crafted MMS client within control system to exploit these vulnerabilities.

Could the vulnerability be exploited remotely?

Yes, an attacker who has network access to control system could use specially crafted MMS client to exploit the vulnerability. However, 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.

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

No.

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.

Will ABB deliver software patches for this vulnerability?

Firmware updates represent an integral part of ABB's life cycle management of Distribution Automation products. ABB will provide the support by delivering the necessary firmware updates according to ABB's Product Life Cycle Management policy. Firmware updates will be available and upcoming patches will be announced at a later stage and this advisory will be updated accordingly.

Support

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

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

Revisions

Rev.	Page (P) Chapt. (C)	Description	Date
A	all	New document	2021-11-29