DOCUMENT ID: 2NGA001147
REVISION: B
DATE: Dec-19-2022

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

The table below describes the products, affected firmware versions, type of fix available and fixed firmware versions.

Product type	Products and Affected Versions	Fix 1 ([1]) / Fix 2 ([2])
Protection and Control Relays	611 series: FW versions prior to 2.0.3	IEC 2.0: FW 2.0.3 [1]
	REF615 IEC 1.0: All existing FW versions	-
	REF615 ANSI 1.0: All existing FW versions	-
	REF615 IEC 1.1: All existing FW versions	-
	RED615 IEC 1.1: All existing FW versions	-
	REF615 ANSI 1.1: All existing FW versions	-
	615 series IEC 2.0: All existing FW versions	-
	615 series CN 2.0: All existing FW versions	-
	615 series ANSI 2.0: All existing FW versions	-
	615 series 3.1 CN: All existing FW versions	-
	615 series IEC 3.0: All existing FW versions	-
	615 series CN 3.0: All existing FW versions	-
	615 series IEC 4.0: All existing FW versions	-
	615 series ANSI 4.0: All existing FW versions	-
	615 series IEC 4.0 FP1: FW versions prior to 4.1.9	IEC 4.0 FP1: FW 4.1.9 [2]
	615 series CN 4.0 FP1: FW versions prior to 4.1.8	CN 4.0 FP1: FW 4.1.8 [2]
	615 series ANSI 4.0 FP1: All existing FW versions	-
	615 series ANSI 4.0 FP2: All existing FW versions	-
	615 series IEC 5.0: FW versions prior to 5.0.12	IEC 5.0: FW 5.0.12 [1]
	615 series IEC 5.0 FP1: FW versions prior to 5.1.20	IEC 5.0 FP1: FW 5.1.20 [2]
	615 series CN 5.0 FP1: All existing FW versions	-
	615 series ANSI 5.0 FP1: All existing FW versions	-
	RER620: All existing FW versions	-
	620 series IEC/CN 2.0: FW versions prior to 2.0.11	IEC/CN 2.0: FW 2.0.11 [1]
	620 series IEC/CN 2.0 FP1: FW versions prior to 2.1.15	IEC/CN 2.0 FP1: FW 2.1.15 [2]
	620 series ANSI: All existing FW versions	-
	REX640 PCL1: FW versions prior to 1.0.8	PCL1: FW 1.0.8 [2]
	REX640 PCL2: FW versions prior to 1.1.4	PCL2: FW 1.1.4 [2]
	REX640 PCL3: FW versions prior to 1.2.1	PCL3: FW 1.2.1 [2]
	REF615R: All existing FW versions	-

Product type	Products and Affected Versions	Fix 1 ([1]) / Fix 2 ([2])
	RER615: FW versions prior to 2.0.3	IEC/ANSI/CN 2.0: FW 2.0.3 [1]
Circuit-Breaker with Integrated Protection	eVD4 equipped with RBX615: All existing FW versions	-
Remote Monitoring and Control	REC615: FW versions prior to 2.0.3	IEC/ANSI/CN 2.0: FW 2.0.3 [1]
Merging Unit	SMU615: FW versions prior to 1.0.2	FW 1.0.2 [2]

The types of fixes

[1] Fix 1: This fix introduces a limitation to the maximum number of concurrent files the MMS client can open. It improves the situation with certain types of MMS clients that are stressing the relay's filesystem, thus causing the Internal Fault "File system error" (Fault code 7). However, in cases where the client is reading files in a fast manner (e.g., once per second), the fault may still appear.

[2] Fix 2: This fix completely solves the problem by modifying the way that the MMS server component is initialized. The original fix 1 is also included in fix 2. The following CVE (Common Vulnerabilities and Exposures) number has been associated: CVE-2021-22283.

Vulnerability ID

ABBID: ABBVREP0060

CVE ID: CVE-2021-22283

Summary

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

ABB had analyzed the problem which was caused when MMS clients attempted to open multiple files without closing them. This eventually blocked other protocols and internal file handling from accessing the file system due to an internal defense mechanism that 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 unless a fix is indicated. Further firmware updates will be announced, and this advisory will be updated accordingly.

Vulnerability severity

The severity assessment was performed 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://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?vector=AV:L/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:F/RL:W/RC:C

Recommended actions

ABB recommends that customers apply the update at their earliest convenience to the products having an updated firmware available.

If unable to update or there is no update available, users should take these defensive measures for minimizing the risk of the MMS file transfer vulnerabilities:

- 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, always use the latest MMS file transfer client software version.
- REX640: Disable MMS access for ports that are not used to access the relay using MMS protocol.

Vulnerability details

The products listed in this advisory have a vulnerability. An attacker could exploit the vulnerabilities by using a specially crafted MMS client, which opens multiple files with file open requests without never closing the files. This would cause the relay to go to an 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 a specially crafted MMS client within the control system to exploit these vulnerabilities.

Could the vulnerability be exploited remotely?

No, the network is typically used only inside a station and must be protected thoroughly. Recommended practices include that process control systems are physically protected, have no direct connections to the Internet, and are separated from other networks through a firewall system with a minimal number of ports exposed. An attacker with network access to the control system network could use a specially crafted MMS client to exploit the vulnerability.

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
B	P2,P3	Revised the list of fixed firmware versions	2022-12-19