DOCUMENT ID: 2NGA001421
REVISION: B
DATE: 2023-05-02

CYBER SECURITY ADVISORY

ABB Relion REX640
Insufficient file access control

CVE ID: CVE-2022-1596

ABBVREP0078

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.

Purpose

ABB has a rigorous internal cyber security continuous improvement process which involves regular testing with industry leading tools and periodic assessments to identify potential product issues. Occasionally an issue is determined to be a design or coding flaw with implications that may impact product cyber security.

When a potential product vulnerability is identified or reported, ABB immediately initiates our vulnerability handling process. This entails validating if the issue is in fact a product issue, identifying root causes, determining what related products may be impacted, developing a remediation, and notifying end users and governmental organizations.

The resulting Cyber Security Advisory intends to notify customers of the vulnerability and provide details on which products are impacted, how to mitigate the vulnerability or explain workarounds that minimize the potential risk as much as possible. The release of a Cyber Security Advisory should not be misconstrued as an affirmation or indication of an active threat or ongoing campaign targeting the products mentioned here. If ABB is aware of any specific threats, it will be clearly mentioned in the communication.

The publication of this Cyber Security Advisory is an example of ABB's commitment to the user community in support of this critical topic. Responsible disclosure is an important element in the chain of trust we work to maintain with our many customers. The release of an Advisory provides timely information, which is essential to help ensure our customers are fully informed.

Affected products

Product type	Products and Affected Firmware (FW) Versions
Protection and Control Relays	REX640 PCL1: FW versions < 1.0.8 REX640 PCL2: FW versions < 1.1.4 REX640 PCL3: FW versions < 1.2.1

Vulnerability ID

CVE-2022-1596

ABBVREP0078

Summary

By exploiting this vulnerability, an authenticated user with any user role could get access to sensitive information, such as user database. While the passwords in the user database are not stored in clear text, they can be subjected to further attacks against the secure hash algorithm.

There is a firmware update available for all firmware levels of the products mentioned in this advisory. If unable to patch the relay, it is recommended to follow the actions described in the mitigating factors chapter.

Recommended immediate actions

The problem is corrected in the following product versions:

- REX640 PCL3: Update the firmware to 1.2.1
- REX640 PCL2: Update the firmware to 1.1.4
- REX640 PCL1: Update the firmware to 1.0.8

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

In case the updated firmware cannot be installed, ABB recommends following the instructions in the Mitigating factors, Workarounds and General security recommendations chapters.

Vulnerability severity and details

A vulnerability exists in the access permissions of the user database file, included in the product versions listed above. An attacker could exploit the vulnerability by retrieving the file with either FTP(S) or HTTP(S) and subject the file to further attacking actions, such as brute force attacking attempts against the hashing algorithm of the passwords or using the usernames for reconnaissance information, etc.

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

CVE-2022-1596

CVSS v3.1 Base Score: 6.5
CVSS v3.1 Temporal Score: 6.2
CVSS v3.1 Vector: AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:F/RL:W/RC:C
NVD Vector Link: https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?vector=AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:F/RL:W/RC:C
NVD Summary Link: https://nvd.nist.gov/vuln/detail/CVE-2022-1596

Mitigating factors

When possible, patch the system with the newest firmware. Refer to section “General security recommendations” for further advise on how to keep your system secure. If unable to patch the system, refer also to the mitigating factors below.

- In local user management mode, use the ABB Protection and Control IED Manager tool PCM600 for re-configuring the user permissions by unchecking the "Read" and "Write" permission checkboxes for all users except Administrator and other possible administrative users, and write the configuration back to the device.

  This mitigation will completely resolve the problem. See the following documents for more information regarding user management and device configuration.

[1] 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.

    - Document ID: 1MRS757866, Revision: G, PCM600 Getting Started Guide
    - Document ID: 1MRS759117, Revision: D, REX640 Engineering Manual
    - Document ID: 1MRS759118, Revision D, REX640 Operation Manual
    - Document ID: 1MRS759122, Revision: D, REX640 Cyber Security Deployment Guideline

- Alternatively, use Central Account Management (CAM), where the problem is not surfacing. See the following documents for more information:
    - Document ID: 1MRS759122, Revision: D, REX640 Cyber Security Deployment Guideline
    - Document ID: 1MRS759142, Revision: F, REX640 Technical Manual
- Do not re-use user credentials between different systems
- Use complex passwords

Workarounds

Although these workarounds will not correct the underlying vulnerability, they can help blocking known attack vectors.

- Limit the HTTP(S) and FTP(S) to a local network by a firewall
- Use a next generation (OSI layer 7) firewall for blocking the traffic to the userdb.xml file
- Disable remote WHMI and FTP(S) and use local HMI only

Frequently asked questions

What is the scope of the vulnerability?

An authenticated attacker who successfully exploited this vulnerability could launch an attack against the user database file and try to take control of an affected system node.

What causes the vulnerability?

The vulnerability is caused by improper access permissions in the user database file in the ABB REX640 protection relay.

What is a user database file?

It is a file which stores the usernames, user roles and hashed (i.e., not in clear text) passwords of the users in ABB REX640 protection relay.

What might an attacker use the vulnerability to do?

An authenticated attacker who successfully exploited this vulnerability could start a second attack against the user database file.

How could an attacker exploit the vulnerability?

The attacker would need to have access to the system network and log in to the device with valid credentials. Recommended practices help mitigate such attacks, see section Mitigating Factors above.

Could the vulnerability be exploited remotely?

Yes, an attacker who has network access and valid user credentials to the 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 completely removes the vulnerability by modifying the access permissions.

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

No, ABB received information about this vulnerability through responsible disclosure. See the Acknowledgement chapter for details.

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.

General security recommendations

For any installation of software-related ABB products we strongly recommend the following (non-exhaustive) list of cyber security practices:

- Isolate special purpose networks (e.g., for automation systems) and remote devices behind firewalls and separate them from any general-purpose network (e.g., office or home networks).
- Install physical controls so no unauthorized personnel can access your devices, components, peripheral equipment, and networks.
- Never connect programming software or computers containing programing software to any network other than the network for the devices that it is intended for.
- Scan all data imported into your environment before use to detect potential malware infections.
- Minimize network exposure for all applications and endpoints to ensure that they are not accessible from the Internet unless they are designed for such exposure and the intended use requires such.
- Ensure all nodes are always up to date in terms of installed software, operating system, and firmware patches as well as anti-virus and firewall.
- When remote access is required, use secure methods, such as Virtual Private Networks (VPNs). Recognize that VPNs may have vulnerabilities and should be updated to the most current version available. Also, understand that VPNs are only as secure as the connected devices.

More information on recommended practices can be found in the following document:

Document ID: 1MRS759122, revision D, REX640 Cyber Security Deployment Guideline

Acknowledgement

ABB thanks Paul Mader and Gianluca Raberger of VERBUND AG's OT Cyber Security Lab for helping to identify the vulnerabilities and protecting our customers.

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 cyber security program and capabilities can be found at www.abb.com/cybersecurity.

Revision history

Rev. Ind.	Page (p) Chapter (c)	Change description	Rev. date
A	all	Initial version	Jun-21-2022
B	p3, c6	Added information regarding fix for REX640 PCL1	May-2-2023