DOCUMENT ID: 2NGA001423
REVISION: A
DATE: 2023-06-12

CYBER SECURITY ADVISORY

ABB Relion REX640
Cyber Security Improvements

CVE ID: CVE-2023-2876, CVE-2011-1473, CVE-2011-3389, CVE-2013-0169

ABBVREP0118

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.

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 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

ABBVREP0118

CVE-2023-2876, CVE-2011-1473, CVE-2011-3389, CVE-2013-0169

Summary

The following vulnerabilities in ABB REX640 has been identified and corrected.

1. In the affected firmware versions listed above, the web server configuration doesn't include setting "HttpOnly" flag in the session cookie. This exposes the WHMI (Web Human-Machine Interface) to cross-site scripting attacks, where potentially sensitive data could be exfiltrated by client-side scripts.
2. In the affected firmware versions listed above, OpenSSL allows client-side renegotiation of the TLS session. This allows an attacker to potentially exhaust the server-side resources, thus causing a DoS (denial of service) attack, where the device is not able to serve legitimate clients.

3. In the affected firmware versions listed above, OpenSSL permits client connections using TLS 1.0 and TLS 1.1 protocol versions. These protocols are considered weak by modern security standards.

Recommended immediate actions

These problems are corrected in the following firmware versions:

- REX640 PCL1: FW version 1.0.8
- REX640 PCL2: FW versions 1.1.4
- REX640 PCL3: FW versions 1.2.1

ABB recommends that customers apply the update at the earliest convenience.
If unable to patch the system, ABB recommends following the instructions in the Mitigating factors, Workarounds and General security recommendations chapters.

Vulnerability severity and details

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

CVE-2023-2876 Sensitive cookie in HTTPS session without "HttpOnly" flag

CVSS v3.1 Base Score: 3.1
CVSS v3.1 Temporal Score: 2.8
CVSS v3.1 Vector: AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C
NVD Vector Link: https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?vector=AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C

CVE-2011-1473 TLS client-side session renegotiation denial of service

CVSS v3.1 Base Score: 5.3
CVSS v3.1 Temporal Score: 4.9
CVSS v3.1 Vector: AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L/E:F/RL:O/RC:C
NVD Vector Link: https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?vector=AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L/E:F/RL:O/RC:C

CVE-2011-3389, Insecure TLS configuration “BEAST”

CVSS v3.1 Base Score: 3.7
CVSS v3.1 Temporal Score: 3.5
CVSS v3.1 Vector: AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N/E:F/RL:O/RC:C
NVD Vector Link: https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?vector=AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N/E:F/RL:O/RC:C

[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.

CVE-2013-0169, Insecure TLS configuration “Lucky 13”

CVSS v3.1 Base Score: 3.7
CVSS v3.1 Temporal Score: 3.5
CVSS v3.1 Vector: AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N/E:F/RL:O/RC:C
NVD Vector Link: https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?vector=AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N/E:F/RL:O/RC:C

Mitigating factors

Refer to section “General security recommendations” for further advice on how to keep your system secure.

Workarounds

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

- Limit the HTTPS and FTPS to a local network by a firewall
- Disable remote WHMI and SFTP, use local HMI only

Frequently asked questions

What is the scope of the vulnerability?

1. **Sensitive cookie in HTTPS session without "HttpOnly" flag vulnerability**
   The vulnerability is related to the web server configuration of the Relion protection relays mentioned above. The attribute " HttpOnly" is not set in the HTTP response header, which means that the session cookie may be accessed by a client-side script.
2. **TLS client-side session renegotiation denial of service vulnerability**
   The vulnerability is related to the OpenSSL version of the Relion protection relays mentioned above. The OpenSSL version used does allow client-side renegotiation of the TLS session and it can be used as a method for creating a denial-of-service attack.
3. **Insecure TLS configuration vulnerabilities**
   The vulnerability is related to the device’s OpenSSL configuration or OpenSSL version that allows the weak TLS 1.0 and TLS 1.1 protocols.

What causes these vulnerabilities?

These vulnerabilities are caused by the web server configuration and OpenSSL version used.

What is cross-site scripting (XSS) and what is a session cookie?

The cross-site scripting (XSS) is an attack technique, where an attacker can inject client-side scripts into a web page, thus possibly leading a legitimate user to a different page or possibly allowing an attacker to circumvent access controls.

A session cookie is a small amount of data containing an identifier that a web server is sending to a client (web browser) for temporary use during a limited timeframe.

What is a denial-of-service attack?

The denial-of-service attack is an attack method, where the attacker sends large amount of data in frequent intervals to a device. When the device tries to handle the requests, it exhausts its resources and thus cannot serve legitimate requests or otherwise perform its functions.

What is TLS (Transport Layer Security)?

TLS is an encryption protocol that provides privacy in webserver-client communication. HTTPS used in connecting REX640 WHMI is an implementation of HTTP protocol with TLS encryption.

What might an attacker use these vulnerabilities to do?

1. **Sensitive cookie in HTTPS session without "HttpOnly" flag**
   The attacker could potentially get sensitive data from the exposed session cookies (e.g., user credentials data) or redirect a legitimate user to a fake login page.
2. **TLS client-side session renegotiation denial of service**
   The attacker could cause a denial-of-service attack by initiating many client-side renegotiation requests, thus rendering the product unresponsive for legitimate HTTPS connections.
3. **Insecure TLS configuration**
   The attacker could exploit weaknesses in older versions of TLS protocol, thus impersonating to be the device itself (i.e., man-in-the-middle attack) or cause a weak cryptographic algorithm to be selected (i.e., a downgrade attack), making it possible to attack against such weak algorithms and compromise the confidentiality of the webserver connection.

How could an attacker exploit the vulnerability?

1. **Sensitive cookie in HTTPS session without "HttpOnly" flag**
   The attacker could e.g., steal the session cookie of a legitimate user and authenticate as that user.
2. **TLS client-side session renegotiation denial of service**
   In an already established connection , the attacker could send multiple client-side renegotiation requests, rendering the web server of REX640 unresponsive for legitimate users.
3. **Insecure TLS configuration**
   The attacker could use released exploit methods for attacking TLS protocol versions 1.0 and 1.1 (such as “Lucky 13” or “BEAST”), thus breaking the confidentiality in REX640’s WHMI traffic.

Could these vulnerabilities be exploited remotely?

Yes, an attacker who has network access to an affected system node could exploit these vulnerabilities, however, the “TLS client-side session renegotiation denial of service” attack requires that the attacker has been first authenticated to the system.

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.

Can functional safety be affected by an exploit of this vulnerability?

1. **Sensitive cookie in HTTPS session without "HttpOnly" flag**
   Only in a case where the attacker would be able to gain access to legitimate privileged user's credentials.

2. **TLS client-side session renegotiation denial of service**
   Yes in case there are important adjacent systems depending on the communication protocols of the relay.
3. **Insecure TLS configuration**
   Yes, in case that the attacker would be able e.g., to inject control commands into the HTTPS stream .

What does the update do?

1. **Sensitive cookie in HTTPS session without "HttpOnly" flag**
   The update adds the "HttpOnly" attribute to the authentication cookie, thus preventing the client-side script accessing the session cookie.
2. **TLS client-side session renegotiation denial of service**
   The update will install a newer version of OpenSSL, where the vulnerability is fixed.
3. **Insecure TLS configuration**
   The update will install a newer version of OpenSSL or reconfigure the OpenSSL so that the weak protocols are not used.

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 C, 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-12-2023