DOCUMENT ID: 2NGA000473
REVISION: C
DATE: 2023-03-27

CYBER SECURITY ADVISORY

Ripple20 impact on Distribution Automation products

CVE ID: CVE-2020-11907, CVE-2020-11909, CVE-2020-11910, CVE-2020-11911, CVE-2020-11912

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

The following table lists the product types, affected products and fixed firmware versions.

Product type	Products and Affected Versions	Fixed in version / Information
Protection and Control Relays	611 series: FW versions prior to 2.0.4	FW 2.0.4
	REF615 IEC 1.0: All existing FW versions	Follow the mitigation instructions
	REF615 ANSI 1.0: All existing FW versions	Follow the mitigation instructions
	REF615 IEC 1.1: All existing FW versions	Follow the mitigation instructions
	RED615 IEC 1.1: All existing FW versions	Follow the mitigation instructions
	REF615 ANSI 1.1: All existing FW versions	Follow the mitigation instructions
	615 series IEC 2.0: All existing FW versions	Follow the mitigation instructions
	615 series CN 2.0: All existing FW versions	Follow the mitigation instructions
	615 series ANSI 2.0: All existing FW versions	Follow the mitigation instructions
	615 series 3.1 CN: All existing FW versions	Follow the mitigation instructions
	615 series IEC 3.0: FW versions prior to 3.0.10	FW 3.0.10
	615 series CN 3.0: All existing FW versions	Follow the mitigation instructions
	615 series IEC 4.0: FW versions prior to 4.0.7	FW4.0.7
	615 series ANSI 4.0: All existing FW versions	Follow the mitigation instructions
	615 series IEC 4.0 FP1: FW versions prior to 4.1.8	FW 4.1.8
	615 series CN 4.0 FP1: FW versions prior to 4.1.7	FW 4.1.7
	615 series ANSI 4.0 FP1: All existing FW versions	Follow the mitigation instructions
	615 series ANSI 4.0 FP2: All existing FW versions	Follow the mitigation instructions
	615 series IEC 5.0: FW versions prior to 5.0.15	FW 5.0.15
	615 series IEC 5.0 FP1: FW versions prior to 5.1.19	FW 5.1.19
	615 series CN 5.0 FP1: FW versions prior to 5.1.1	FW 5.1.1
	615 series ANSI 5.0 FP1: FW versions prior to 5.1.2	FW 5.1.2

Product type	Products and Affected Versions	Fixed in version / Information
	RER620: All existing FW versions	Follow the mitigation instructions
	620 series IEC/CN 2.0: FW versions prior to 2.0.12	FW 2.0.12
	620 series IEC/CN 2.0 FP1: FW versions prior to 2.1.13	FW 2.1.13
	620 series ANSI: FW versions prior to 2.0.3	FW 2.0.3
	REX640 PCL1: FW versions prior to 1.0.6	FW 1.0.6
	REX640 PCL2: FW versions prior to 1.1.2	FW 1.1.2
	REF615R: All existing FW versions	Follow the mitigation instructions
	RER615: FW versions prior to 2.0.7	FW 2.0.7
Circuit-Breaker with Integrated Protection	eVD4 equipped with RBX615: All existing FW versions	Follow the mitigation instructions
Remote Monitoring and Control	REC615: FW versions prior to 2.0.7	FW 2.0.7
Merging Unit	SMU615: FW versions prior to 1.0.2	FW 1.0.2

Vulnerability IDs

CVE-2020-11907, CVE-2020-11909, CVE-2020-11910, CVE-2020-11911, CVE-2020-11912

ABBVU-116050

Summary

ABB is aware of public reports of a vulnerability in the product versions listed above. On the 16th of June 2020, a series of vulnerabilities affecting a TCP/IP library from Treck Inc. were made public by JSOF Tech in Jerusalem, Israel. The products listed in this document have integrated this library and thus are affected by the vulnerabilities listed in this document.

The products listed in this document are affected by the vulnerability described in this document unless a fix is indicated. When further firmware updates will be announced, this advisory will be updated accordingly.

An attacker who successfully exploited this vulnerability could make the product inaccessible, cause delays in network connection or detect the software version of the device.

Recommended immediate actions

The problem is corrected in the products listed in the table above, where the fixed firmware is stated. ABB recommends that customers apply the update at earliest convenience.

For products that haven't yet received a firmware update (marked in the table as "All existing FW versions"), ABB recommends following the chapter "Mitigating factors".

Vulnerability severity and details

A vulnerability exists in the TCP/IP library included in the product versions listed above. An attacker could exploit the vulnerability by sending a specially crafted message to the system node, causing the node to become inaccessible, causing the node to reveal version information or causing the node to respond in a slow manner.

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

CVE IDs and vulnerability descriptions

CVE-2020-11907
CVSS v3.1 Base Score: 6.3 (high)
CVSS v3.1 Temporal Score: 5.9
CVSS v3.1 Vector: AV:A/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L/E:F/RL:O/RC:C
CVSS v3.1 Vector Link: https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?vector=AV:A/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L/E:F/RL:O/RC:C
NVD Summary Link: https://nvd.nist.gov/vuln/detail/CVE-2020-11907
Effect: This vulnerability may cause Denial of Service to TCP connections.
Mitigation: Can be mitigated by a firewall device or NAT device that inspects TCP options, rejecting any malformed packets.

CVE-2020-11909
CVSS v3.1 Base Score: 5.3 (medium)
CVSS v3.1 Temporal Score: 4.9
CVSS v3.1 Vector: AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:F/RL:O/RC:C
CVSS v3.1 Vector Link: https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?vector=AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:F/RL:O/RC:C
NVD Summary Link: https://nvd.nist.gov/vuln/detail/CVE-2020-11909
Effect: Attacker may use this vulnerability to detect the software version of the device.
Mitigation: Can be mitigated by blocking various IP source routing.

CVE-2020-11910
CVSS v3.1 Base Score: 5.3 (medium)
CVSS v3.1 Temporal Score: 4.9
CVSS v3.1 Vector: AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:F/RL:O/RC:C
CVSS v3.1 Vector Link: https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?vector=AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:F/RL:O/RC:C
NVD Summary Link: https://nvd.nist.gov/vuln/detail/CVE-2020-11910
Effect: This vulnerability may cause delays to UDP/TCP connections
Mitigation: Can be mitigated by blocking ICMP MTU update message.

CVE-2020-11911
CVSS v3.1 Base Score: 5.3 (medium)
CVSS v3.1 Temporal Score: 4.9
CVSS v3.1 Vector: AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/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.

CVSS v3.1 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:L/A:N/E:F/RL:O/RC:C
NVD Summary Link: https://nvd.nist.gov/vuln/detail/CVE-2020-11911
Effect: This vulnerability may cause Denial of Service to UDP/TCP connections.
Mitigation: Can be mitigated by blocking ICMP Address Mask Reply message.

CVE-2020-11912
CVSS v3.1 Base Score: 5.3 (medium)
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
CVSS v3.1 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
NVD Summary Link: https://nvd.nist.gov/vuln/detail/CVE-2020-11912
Effect: This vulnerability may cause Denial of Service to TCP connections.
Mitigation: Can be mitigated by a firewall device or NAT device that inspects TCP options, rejecting any malformed packets.

Mitigating factors

To minimize the risk of the Ripple20 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 a firewall, NAT device to block
    - malformed TCP/IP packets
    - IP source routing
    - ICMP Address Mask Reply and MTU update messages

It is recommended to have all assets updated with the latest firmware and security patches.

Firmware updates can be downloaded from the following link: https://protection.datacare.abb.com/

In addition, refer to section “General security recommendations” for further advise on how to keep your system secure.

Frequently asked questions

What is the scope of these vulnerabilities?

The scope is network-bound, these vulnerabilities are related to the TCP/IP stack of the device. An attacker who successfully exploited this vulnerability could block the TCP/IP communication to the SCADA system.

What causes these vulnerabilities?

The vulnerabilities are caused by the following flaws in the TCP/IP stack implementation.

CVE-2020-11907

The Treck TCP/IP stack before 6.0.1.66 improperly handles a Length Parameter Inconsistency in TCP.

CVE-2020-11909

The Treck TCP/IP stack before 6.0.1.66 has an IPv4 Integer Underflow.

CVE-2020-11910

The Treck TCP/IP stack before 6.0.1.66 has an ICMPv4 Out-of-bounds Read.

CVE-2020-11911

The Treck TCP/IP stack before 6.0.1.66 has Improper ICMPv4 Access Control.

CVE-2020-11912

The Treck TCP/IP stack before 6.0.1.66 has a TCP Out-of-bounds Read.

What is Treck TCP/IP library?

It is a software component that implements the TCP/IP connectivity stack of the device.

What might an attacker use these vulnerabilities to do?

An attacker who successfully exploited these vulnerabilities could prevent legitimate access to an affected system node (e.g., cause the TCP/IP communication to the SCADA system to stop or become inaccessible), cause delays in network connection or detect the software version of the device. However, the protection functions and GOOSE communication will not be affected.

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 system node. 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. 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 exposed.

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

Yes, the attacker could e.g., stop the legitimate users remotely operating switching objects by exploiting these vulnerabilities.

What does the update do?

The update completely removes these vulnerabilities by modifying the way that the TCP/IP stack handles the traffic.

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

Yes, these vulnerabilities have been publicly disclosed.

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 documents:

1MRS758337, 611 series Cyber Security Deployment Guideline, revision B

1MRS758280, 615 series Cyber Security Deployment Guideline, revision C

1MRS758294, 620 series Cyber Security Deployment Guideline, revision B

1MRS759122, REX640 Cyber Security Deployment Guideline, revision D

1MRS758410, Substation Merging Unit SMU615 Cyber Security Deployment Guideline, revision B

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	2020-07-31
B		Firmware updates	2021-08-27
C		Firmware updates	2023-03-27