DOCUMENT ID: 2NGA000473
REVISION: A
DATE: 2020-07-31

CYBERSECURITY 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.

# Affected products

| Product type | Products and Affected Versions |
|---|---|
| Protection and Control Relays | 611 series: All existing firmware versions<br>615 series: All existing firmware versions<br>620 series: All existing firmware versions<br>REX640: All existing firmware versions<br>REF615R: All existing firmware versions<br>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 |
| Feeder Terminal | REF542 plus with option E or F communication module (1VCR009634001, 1VCR009634002) : All existing firmware versions |
| Communication Adapter | SPA-ZC 400 rev C: Firmware version 2.0 and later<br>SPA-ZC 402 rev C : Firmware version 2.0 and later |

# Vulnerability ID

ABBID: ABBVU-116050-Ripple20

# Summary

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. Firmware updates will be announced at a later stage and this notification will be updated accordingly.

# Vulnerability severity

The severity assessment has been performed by using the FIRST Common Vulnerability Scoring System (CVSS) v3. 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 v3.0 Base Score: | 7.3 (High) |
| CVSS v3 Temporal Score: | 6.5 (Medium) |
| CVSS v3 Vector: | CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L/E:U/RL:W/RC:C |
| CVSS v3 Link: | https://www.first.org/cvss/calculator/3.0#CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L/E:U/RL:W/RC:C |

# Recommended actions

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.

# Vulnerability details

The products listed above use the vulnerable TCP/IP stack. An attacker could exploit the vulnerabilities by sending specially crafted messages via the Ethernet Network.

ABB has analyzed the vulnerabilities of the Ripple20 vulnerability set. Due to the configuration of the stack these 5 out of 19 vulnerabilities are affecting the devices:

**CVE-2020-11907**

| | |
|---|---|
| NVD CVSS3.1 score: | 6.3 (high) |
| NVD-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**

| | |
|---|---|
| NVD CVSS3.1 score: | 5.3 (medium) |
| NVD-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**

NVD CVSS3.1 score: 5.3 (medium)
NVD-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**

NVD CVSS3.1 score: 5.3 (medium)
NVD-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**

NVD CVSS3.1 score: 5.3 (medium)
NVD-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.

# Frequently asked questions

**What is the scope of the vulnerability?**

An attacker who successfully exploited this vulnerability could block the TCP/IP communication to the SCADA system. The protection functions and GOOSE communication will not be affected.

**What causes the vulnerability?**

The vulnerability is caused by a flaw in the TCP/IP stack integrated into the devices.

**What might an attacker use the vulnerability to do?**

An attacker who successfully exploited this vulnerability could cause the TCP/IP communication to the SCADA system to stop or become inaccessible.

**How could an attacker exploit the vulnerability?**

An attacker must send special crafted malformed IP packages to exploit these vulnerabilities.

**Could the vulnerability be exploited remotely?**

Yes, an attacker who has network access can send special frames via the network to exploit the 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.

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

Yes, this vulnerability has been publicly disclosed by the JSOF institute.

**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 announced in later stage and this notification will be updated accordingly.

# Acknowledgement

ABB thanks JSOF for helping to identify the vulnerabilities and protecting our customers.

# References

https://www.jsof-tech.com/ripple20/

# 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 | 2020-07-31 |
| | | | |
| | | | |