CYBER SECURITY NOTIFICATION

Cyber Security Notification

Ripple20 Vulnerabilities, impact on ABB products

Release date: 15.7.2020

Update date: 14.8.2020

Notice

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 announcement states that a variety of products have integrated this library and thus are affected by one or more of the Common Vulnerabilities and Exposures (CVEs) listed below.

ABB is evaluating the potential impacts on a number of products and has initiated our vulnerability handling process to ensure any product related issues are properly addressed. With this announcement from JSOF Tech it is understood that ABB will need to integrate patches or fixes to address these vulnerabilities in the Treck Inc software for products which are affected, according to the ABB Vulnerability Handling policy. We are currently analyzing our product portfolio for exposure. Potentially affected customers should expect additional communication or advisories as more details become available.

The vulnerability CVE numbers and CVSS scores are listed in the table below:

CVE	CVSSv3 Score
CVE-2020-11896	10
CVE-2020-11897	10
CVE-2020-11901	9
CVE-2020-11898	9.1
CVE-2020-11900	8.2
CVE-2020-11902	7.3
CVE-2020-11904	5.6
CVE-2020-11899	5.4
CVE-2020-11903	5.3
CVE-2020-11905	5.3
CVE-2020-11906	5
CVE-2020-11907	5
CVE-2020-11909	3.7
CVE-2020-11910	3.7
CVE-2020-11911	3.7
CVE-2020-11912	3.7
CVE-2020-11913	3.7
CVE-2020-11914	3.1
CVE-2020-11908	3.1

Affected Products

The products listed in the table are affected by the vulnerabilities listed. ABB continues to evaluate the vulnerabilities and will update the advisory when additional information becomes available

Product / System line	Products and Affected Versions	Link to Advisory
Protection and Control Relays	611 series: All existing firmware versions 615 series: All existing firmware versions 620 series: All existing firmware versions REX640: All existing firmware versions REF615R: All existing firmware versions RER615: All existing firmware versions	Advisory
Circuit-Breaker with Integrated Protection	eVD4 equipped with RBX615: All existing firmware versions	Advisory
Remote Monitoring and Control	REC615: All existing firmware versions	Advisory
Merging Unit	SMU615: All existing firmware versions	Advisory
Feeder Terminal	REF542 plus with option E or F communication module (1VCR009634001, 1VCR009634002) : All existing firmware versions	Advisory
Communication Adapter	SPA-ZC 400 rev C: Firmware version 2.0 and later SPA-ZC 402 rev C : Firmware version 2.0 and later	Advisory
Connected Services	Service Box 1st generation, DSQC 680: All existing variants (GPRS, Wired, 3G) and firmware versions.	

ABB products not listed are initially evaluated as not impacted. We will continue the investigation and update the table if products are identified as affected.

Mitigation Factors

Recommended security practices and firewall configurations can help protect an industrial control network from attacks that originate from outside the network. Such practices include ensuring that protection, control & automation systems are physically protected from direct access by unauthorized personnel, 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, and others that have to be evaluated case by case. In general protection, control & automation systems should not be used for general business functions which are not critical industrial processes. Portable computers and removable storage media should be carefully scanned for viruses before they are connected to a control system. Block all non-trusted IP communications.

To minimize the risk of exploitation of the Ripple20 vulnerabilities users should take these defensive measures:

- Locate the control system network behind a firewall and separate them from other networks.
- Block anomalous IP traffic by utilizing a combination of firewalls and intrusion prevention systems.
- Disable or block IP tunneling, both IPv6-in-IPv4 or IP-in-IP tunneling.
- Avoid exposure of the devices to the Internet and use secure methods like VPN when accessing them remotely.

Support

For additional information and support please contact your product provider or ABB service organization. For contact information, see http://new.abb.com/contact-centers. Information about ABB's cyber security program and capabilities can be found at www.abb.com/cybersecurity.