Health-ISAC Vulnerability Bulletin

TLP:WHITE

Date: June 19, 2020

Event: Ripple20 Treck TCP/IP Stack Vulnerability

Summary

Ripple20 is a host of zero-day vulnerabilities discovered in a low-level TCP/IP software library developed by a software company called Treck. The stack of vulnerabilities, discovered by Israel-based security company JSOF, affects millions of devices and includes remote code execution (RCE) vulnerabilities. The vast risks associated with this vulnerability impacts products such as smart home devices, power grid equipment, healthcare systems, printers, routers, data center devices, and many more. Ripple20 can cause data to be stolen from printers, abnormal or inconsistent infusion pump behavior, and industrial control devices to malfunction.

The large scope of impacted products is due to the consistent implementation of the software library. Issues surrounding Ripple20 are exacerbated as the vulnerable software was not only used by equipment vendors directly but also integrated into other software suites, further complicating the response as device manufactures may be unaware of the underlying code in the software libraries they use.

Identifying all the vulnerable devices is not yet done. Researchers derived the name Ripple20 as the, currently amounted, 19 vulnerabilities are expected to cause a ripple effect in the IoT landscape in 2020, and the years to come. As the search continues, researchers have only scratched the surface of discovering all the devices that have employed the vulnerable TCP/IP library. Of the 19 vulnerabilities, four (CVE-2020-11896, CVE-2020-11897, CVE-2020-11898, and CVE2020-11899), have critical ratings of 10 and 9.8 by the US Department of Homeland Security on the CVSSv3 vulnerability severity scale.

Analysis & Action

When the four critical vulnerabilities are weaponized, attackers can take control of smart devices or any industrial or health care equipment. Attacks are possible via the internet if the devices are connected online, or from local networks if the attacker gains a foothold on an internal network. According to research, the four vulnerabilities are ideal for both botnet operators, as well as targeted attacks.

Ripple20 poses significant risks to devices implementing unpatched versions of the Treck TCP/IP Stack. Once adversaries gain access to network devices, they can execute crafty malicious attacks. Potential risk scenarios include:

- An attacker from outside the network taking control over a device within the network, if internet facing.
- An attacker who has already managed to infiltrate a network can use the library vulnerabilities to target specific devices within it.
- An attacker could broadcast an attack capable of taking over all impacted devices in the network simultaneously.
- An attacker may utilize an affected device to remain hidden within the network for years
- A sophisticated attacker can potentially perform an attack on a device within the network, from outside the network boundaries, thus bypassing NAT configurations. This can be done by performing a MITM attack or a DNS cache poisoning.
- In some scenarios, an attacker may be able to perform attacks from outside the network by replying to packets that leave network boundaries, bypassing NAT

The impact of the Ripple20 vulnerabilities is expected to be the same as the Urgent/11 vulnerabilities. The resemblance is attributed to the impact the Urgent/11 vulnerabilities had on the TCP/IP networking stack of the VxWorks real-time operating system. This was also a product widely used in the IoT and industrial landscape.

Mitigations

H-ISAC recommends users apply the latest version of the affected products. The following recommended mitigations should be implemented:

- Minimize network exposure for all control system devices and/or systems and ensure that they are not accessible from the Internet. The Ripple20 security issues could provide additional justification for internal network segmentation.
- Locate control system networks and remote devices behind firewalls and isolate them from the business network.
- When remote access is required, use secure methods, such as Virtual Private Networks (VPNs), recognizing that VPNs may have vulnerabilities and should be updated to the most current version available. Also recognize that VPN is only as secure as the connected devices.
- Use an internal DNS server that performs DNS-over-HTTPS for lookups.

More detailed information on the vulnerabilities and mitigating controls can be found here. Organizations are recommended to perform proper analysis and risk assessment prior to deploying defensive measures.

Medical Device Manufacturer Security Updates

At the time of this publication, the following Medical Device Manufacturers have issued security patches to address the Ripple20 vulnerabilities.

Manufacturer	Public Advisory
B. Braun	https://www.bbraunusa.com/en/products-and-therapies/customer-communications.html
Baxter	https://www.baxter.com/product-security
Carestream	https://www.carestream.com/en/us/services-and-support/cybersecurity-and-privacy
GE Healthcare	https://www.gehealthcare.com/security
Medtronic	https://global.medtronic.com/xg-en/product-security/security-bulletins.html

The Health-ISAC site web page here (https://h-isac.org/mdm-security/) provides access to medical device manufacturers' product security websites. The URLs for each manufacturer on the page will link to their product security site where you will find relevant security information.

Medical Device Security Media Education Materials

The following is an excerpt from Health-ISAC set of media education materials covering broad medical device security, including the coordinated vulnerability disclosure process for medical devices. The materials include Media Education Materials and the Coordinated Vulnerability Disclosure Process. The media education materials are located on the Health-ISAC website here: https://h-isac.org/cvd-media-kit/.

The cyber security threat landscape has evolved, and many industries are impacted. Medical device manufacturers are often working to manage fielded, supported devices (those that are currently in use in hospitals, clinics, or patient homes and still supported by the manufacturer) that are critical to delivering therapy. As the landscape evolves, those products need updating. Newer products have more rigid security standards because they are developed in a time when expectations specifically regarding security and the ability to update are different.

- Security vulnerabilities are not unique to the medical device industry. Everyone with a smart phone installs periodic software updates when they are released (typically several times a year). Some automotive companies update their products over the air, without requiring drivers to make a trip for a fix. Even television sets download and update software from time to time. Medical devices also need to be updated as technology evolves. The medical device industry is no different than other Internet of Things ("IOT") devices.
- Disclosures, and increased transparency, are a sign of increased company responsibility and accountability– not an admission of fault. Many organizations operating in high-tech fields are issuing security vulnerability notices.
- Most companies follow coordinated disclosure processes (see separate coordinated vulnerability disclosure document - LINK) that encourage transparency in the communication of

vulnerable products to the clinician and patient community. These processes, which may be documented on a company's external website, guide the steps taken when a security concern is identified and helps ensure that the matter is communicated and addressed in a transparent way.

References

- Ripple20 Vulnerabilities Affecting Treck IP Stacks https://www.us-cert.gov/ncas/current-activity/2020/06/16/ripple20-vulnerabilities-affecting-treck-ip-stacks
- Ripple20 19 Zero-Day Vulnerabilities Amplified by the Supply Chain https://www.jsof-tech.com/ripple20/
- Ripple20 vulnerabilities will haunt the IoT landscape for years to come https://www.zdnet.com/article/ripple20-vulnerabilities-will-haunt-the-iot-landscape-for-years-to-come/
- ICS Advisory (ICSA-20-168-01) https://www.us-cert.gov/ics/advisories/icsa-20-168-01
- Health Industry Cybersecurity Practices (HICP): Managing Threats and Protecting Patients publication https://healthsectorcouncil.org/hhs-and-hscc-release-voluntary-cybersecurity-practices-for-the-health-industry/
- Health-ISAC Medical Device Manufacturers' Product Security Websites https://h-isac.org/mdm-security/
- Health-ISAC Medical Device Security Media Education Materials https://h-isac.org/cvd-media-kit/

For questions or comments, please email us a toc@h-isac.org
Health-ISAC Threat Operations Center
100 Boeing Way Suite 1200, Titusville, FL 32780
(321) 593-1470
www.h-isac.org

This e-mail is intended only for the individual(s) or entity(s) named within the message. This email might contain privileged or confidential information. If the reader of this message is not the intended recipient(s), or the agent responsible to deliver it to the intended recipient, you are hereby notified that any review, dissemination, distribution of this communication is prohibited by the sender. To do so might constitute a violation of the Electronic Communications Privacy Act., U.S.C. Section 2510-2521.