Exploit Research and Presentation: Ripple20

Levi Overstreet

University of Advancing Technology: NTS330

Exploit Research and Presentation: Ripple20

An exploit is usually a code that take advantage of a software or hardware vulnerability or security flaw. These codes are written either by security researchers as proof-of-concept threat or by malicious actors for use in their operations. When used, some exploits can allow an intruder to remotely access a network and gain elevated privileges or move deeper into the network. In some cases, an exploit can be used as a part of a multi-component attack or to simply propagate the malicious code and infect as many systems as possible. This paper will answer the question; what is Ripple20?

Background

Ripple20 is a set of 19 vulnerabilities in a software library that implemented a TCP/IP stack. These vulnerabilities were discovered in June of 2020 by researchers from JSOF. The security concerns are centered around the fact that potentially tens of millions of devices that utilize the popular Treck embedded TCP/IP stack are affected. Several of the vulnerabilities, with CVSS scores over 9, critically impact the device or system with Remote Code Execution and exposure of sensitive information (Forescout, 2020).

Impact

The level of impact is the reason this group of vulnerabilities was given its name. JSOF coined the name due to the incredible extent of impact which is magnified by the supply chain factor. The wide-spread dissemination of the software library, and its internal vulnerabilities, was a natural consequence of the supply chain "ripple-effect" (JSOF, 2020). The reason for this massive proliferation is because the software library in question was provided by Treck Inc, a large supplier of embedded TCP/IP software.

Treck Inc. & IoT

According to their website, Treck Inc. has been designing, distributing and supporting real-time embedded Internet protocols for worldwide technology leaders since 1997 (Treck, 2020). Due to the increased demand and production of IoT devices, the need for embedded TCP/IP also increased. This allowed Treck’s software to be distributed to a large footprint within the IoT manufacturing in many different industries. To the credit of Treck Inc, they have released patches for all 19 vulnerabilities, which can be found on their website. But the fact that this software, which was released in the late nineties, has been available and in use for many years and enterprises of all sizes have been bringing more and more devices online, it is no surprise that the impact of Ripple20 is so widespread.

Mitigation and Solutions

Detection is the first step to avoiding attacks that abuse these vulnerabilities. In some cases, asset owners may not be aware that these vulnerabilities exist in their environment. Upon detection of vulnerabilities, if any, users should immediately apply the security updates supplied by the manufacturer which requires patching all devices running the vulnerable version of the IP stack. This is not easy because devices with embedded systems are notoriously difficult to manage and update since traditional endpoint agents cannot be installed, and updates usually require a firmware reflash (dos Santos, 2020). But luckily many security software providers, such as Trend Micro and Forescout, have been supplying solutions to help detect the devices affected, segment them from systems or networks for control and quarantine, and to assist in the process of patching and flashing as needed.

The prevalence of so many vulnerabilities across hundreds of millions of devices for years shows just how messy the interdependent security ecosystem for the internet of things remains. Without an agreed standard or strict quality control in place, these kinds of problems will continue to show that we need to fix the current system. Hopefully sooner, rather than later.

References

dos Santos, Daniel. (2020). Identifying and Protecting Devices Vulnerable to Ripple20. Retrieved from https://www.forescout.com/company/blog/identifying-and-protecting-devices-vulnerable-to-ripple20/

Forescout. (2020). Ripple20 Vulnerabilities. Retrieved from https://www.forescout.com/company/resources/ripple20-vulnerabilities/

JSOF. (2020). Ripple20: 19 Zero-Day Vulnerabilities Amplified by the Supply Chain. Retrieved from https://www.jsof-tech.com/ripple20/

Treck. (2020). Welcome to TRECK. Retrieved from https://treck.com/