harborlabs
CYBER. SCIENCE

CYBERVIGILANCE ALERT

Ripple20

CVSS: 10

Harbor Labs has been actively following the Ripple20 suite of vulnerabilities identified and released by LSOF. Based on their findings and ongoing collaborations with LSOF, Harbor Labs is issuing the following alert.

The 19 reported vulnerabilities associated with Ripple20 range from medium-to-critical per CVSS severity scoring guidelines. In the most severe cases, an attacker may perform remote code execution, which gives the attacker complete control of the device. Harbor Labs has reviewed the technical documentation provided by LSOF and understand that the vulnerability is due to an incorrect conditional statement executed when handling IP packet fragmentation. This single error, when exploited, creates a number of memory-related errors that can then be further exploited. The crux of the attack relies on IP-in-IP encapsulation. IP encapsulated and fragmented packets are easily fabricated using open source software like *Scapy*.

These vulnerabilities affect the Treck TCP/IP stack, a software implementation or library used by a large number of embedded systems and IoT products. The authors, LSOF, specifically cite infusion pumps and industrial control systems as potential affected targets, but the vulnerability has the potential to affect a wide variety of medical devices and healthcare IoT systems.

Harbor Labs has noted that IP tunneling is required to exploit the vulnerability. This does not mean that the threat model must only consider IP-in-IP tunneling from an external source over the Internet. It is possible to generate arbitrary IP-in-IP packets using tools such as Scapy by any user on the internal network.

Please review the characteristics of this vulnerability to determine whether this could impact one of your devices. The Harbor Labs staff is fully versed in the vulnerability and associated exploits, and are working with LSOF to utilize their validation script. We are standing by should you require any assistance in determining how you are affected, or in implementing any necessary remediation.