Ripple20: A mission-critical risk

A series of vulnerabilities in a common networking stack underscores the need for device visibility

Erik Floden
Director, Federal Civilian Agencies,
Forescout Technologies

RESEARCHERS RECENTLY UNCOVERED a new threat that poses unique risks to mission-critical devices. Ripple20 is a series of 19 vulnerabilities, including multiple remote code execution vulnerabilities, in a low-level TCP/IP software library developed by a company named Treck. That piece of software is embedded in a wide range of devices.

Forescout worked with JSOF, which first uncovered Ripple20, to identify the devices and vendors impacted by these vulnerabilities. JSOF estimates that hundreds of millions of internet of things and operational technology (OT) devices are at risk, and they are as varied as printers, uninterruptible power supplies, medical infusion pumps and industrial control systems. In short, Ripple20 can disrupt mission-critical technology that security teams typically don't spend much time managing and sometimes can't manage because the embedded software is not accessible.

Unfortunately, that means there is no single manufacturer with a practiced way to fix the software. Instead, the burden falls on security teams to understand and mitigate the risk.

How to minimize the threat

Ripple20 is a perfect example of the importance of being able to classify, segment, assess and enforce control actions. To tackle the risk, government security teams should:

1. **Identify all vulnerable devices.** Unfortunately, many agencies don't know all the devices connected to their networks. But that needs to change because the inability to identify characteristic network signatures of devices using Treck can be a huge weakness.

2. **Apply a patch from the device's vendor.** When a patch is delayed or not available, agencies must be able to limit or segment the device's access until it can be patched.

3. **Continuously monitor the behavior of a vulnerable device** until a patch is ready. Real-time, granular visibility is essential to ensure that the device is not compromised and acting maliciously.

4. **Automate response and remediation workflows** as patches are issued. Otherwise, agencies will spend precious time manually mitigating the vulnerability.

Converging security strategies

Risks like Ripple20 will only increase as IoT devices continue to spread across networks. In addition, such vulnerabilities are affecting both traditional IT and OT.

Fortunately, we have also begun to see a convergence in security leadership for both types of technology, rather than having two separate security teams.

Although the types of security applied to IT networks might be slightly different for OT networks, it's critically important that agencies take a close look at their entire IT environments as soon as possible. Ripple20 is a severe risk, and it is likely just the beginning. ■

Erik Floden is director of federal civilian agencies at Forescout Technologies.