FORESCOUT

Ripple20 Vulnerabilities

FAQ: Identify & Mitigate Risk with Forescout

Q: What is Ripple20?

A: Ripple20 is a set of 19 vulnerabilities, potentially affecting tens of millions of devices utilizing the popular Treck embedded TCP/IP stack. Ripple20 was disclosed by the cybersecurity research company JSOF. Four of the vulnerabilities have a critical CVSS score, with impact including Remote Code Execution (RCE) and exposure of sensitive information. Learn more here.

CERT/CC advisory: https://kb.cert.org/vuls/id/257161
ICSA advisory: https://www.us-cert.gov/ics/advisories/icsa-20-168-01

Q: Is my organization vulnerable?

A: It is highly likely that you have devices vulnerable to Ripple20. The Treck embedded TCP/IP stack is widely used by companies such as HP, Intel, Schneider Electric, DIGI and many others to create products that range from home and enterprise printers to Industrial Control Systems (ICS) and healthcare equipment. Research from Forescout Device Cloud found a wide variety of devices running the Treck embedded TCP/IP stack, with healthcare, retail, financial, government and manufacturing being the most impacted verticals. Common device types running Treck embedded TCP/IP stack include infusion pumps, printers, UPS systems, networking equipment, point of sale devices, IP cameras, video conferencing systems, building automation devices and ICS devices. Devices such as IP cameras and printers can be found in nearly every enterprise, creating a potential security exposure.

Q: How does it impact devices?

A: To exploit Ripple20 vulnerabilities, an attacker needs a direct connection to a vulnerable device or a routed path to internal networks. This means devices directly connected to the internet are those most at risk. An attacker could target vulnerable devices, compromise them and move laterally within the network to access or infect other devices.

The Ripple20 vulnerabilities will allow for RCE which potentially allows for data exfiltration or replacing the firmware with a malicious one. If exploited in such a fashion, these vulnerabilities may allow an attacker to remain hidden and persistent in an enterprise network for years of surveillance, data exfiltration, malware deployment, etc.

Q: Can Forescout help identify vulnerable devices?

A: Yes. Forescout has released a Security Policy Template (SPT) for eyeSight and eyeControl which helps organizations detect potentially vulnerable devices by flagging the characteristic network signatures of devices using the Treck embedded TCP/IP stack. Forescout will continue to refine this template as the situation evolves and additional information becomes available.

For OT networks, Forescout has released a SilentDefense SD script which provides custom detection for active exploitation of the most critical vulnerabilities so that mitigation steps can be taken once an active attack is detected.

Q: I am a Forescout eyeSight customer. Is there an SPT to identify vulnerable devices?

A: Yes. As mentioned above, Forescout has released a SPT that identifies devices in your environment that are potentially vulnerable to Ripple20. Vulnerable devices are categorized as Very High, High and Medium certainty levels so appropriate mitigation actions can be taken. Vulnerabilities are found using a combination of passive and active techniques such as DHCP fingerprinting, TCP fingerprinting, compromised device vendor lookup, NMAP and ICMP scans.

Q: What eyeSight techniques do I need to use to find vulnerable devices?

A: Forescout uses a combination of passive and active techniques to give you the flexibility and greater degree of certainty in detecting vulnerable devices. These include passive techniques such as DHCP fingerprinting, TCP fingerprinting, compromised device vendor lookup and active techniques such as NMAP and ICMP scans. While not all techniques need to be enabled, multiple vectors of assurance provide a higher degree of confidence.

For sensitive environments, such as those with medical IoTs, passive-only techniques should be used. For smaller remote sites that often can't provide SPAN traffic, techniques such as DHCP fingerprinting, NMAP and ICMP scans are available for full visibility into vulnerable devices across all parts of the network.

Q: Can I patch vulnerable devices?

A: Some vendors have made patches available. However, there are other complicating factors. Due to the challenges with supply chain vulnerabilities and embedded components as described in this blog, the vendor that creates the patch isn't necessarily the one that will release it. This can delay the issuance of a patch.

There are also no guarantees that the device vendor is still in business so a patch may never be available. The complex nature of the supply chain may also mean the device is not patchable at all, even if it needs to remain on the network. Additionally, many of the affected devices are part of critical operations and infrastructure that may necessitate patching only during planned maintenance windows. In all such cases, mitigation controls such as segmentation should be the first line of defense. Segmentation can limit the likelihood of compromise and the impact of compromise (blast radius) without disrupting critical systems and business operations.

Q: How else do I mitigate risks from Ripple20?

A: There are multiple ways to reduce the risk associated with Ripple20 vulnerabilities. Following defense in depth principles it is advisable to adhere to as many of these risk mitigation methods as is feasible.

- First and foremost, use Forescout eyeSight with its newly released SPT policies to identify all potentially vulnerable devices across all parts of the network. Forescout categorizes the vulnerable devices into Very High, High and Medium certainty levels helping set the foundation for mitigation controls. For OT networks, use the newly released SD script from SilentDefense that provides custom detection for the most critical vulnerabilities. Additionally, use SilentDefense to detect active exploitation of these vulnerabilities so mitigation steps can take place once an active attack is detected.
- Once Forescout eyeSight has identified potentially vulnerable devices, customers should logically group those assets to form the basis for segmentation-based mitigation. It's important to take the business function of the asset into consideration while logically grouping devices, as the mitigation actions on a printer may be different than a business critical IoT device. At that point, customers can use eyeSegment and eyeControl to detect and block anomalous IP traffic; and apply segmentation controls to decrease the communication allowed to/from these potentially vulnerable devices, thereby limiting the likelihood of compromise and the blast radius if a compromise occurs.
- In addition to immediately reducing risk by taking mitigation actions, customers should continuously monitor the traffic to and from these high-risk devices. Forescout eyeSegment monitors the ongoing traffic and behavior of the device, so when anomalous traffic flows are detected, response actions or more stringent controls can be enforced.

Q: I am a Forescout SilentDefense customer. Can I detect Ripple20 vulnerabilities on my OT network?

A: Yes. SilentDefense already detects problematic network communications, anomalies, and malformed packets. To identify Ripple20 vulnerabilities, Forescout has released an SD script that provides custom detection for the most critical Ripple20 vulnerabilities, including CVE-2020-11896, CVE-2020-11897, CVE-2020-11898, CVE-2020-11901, CVE-2020-11903, CVE-2020-11909, CVE-2020-11910, and CVE-2020-11911. Additionally, SilentDefense can also detect active exploitation of these vulnerabilities so critical alerts/mitigation steps can take place once an active attack is detected.

As affected vendors release their own security advisories, the SilentDefense CVE database will continue to be updated with latest vulnerabilities.

Note: The SD script detects potentially vulnerable devices using passive DHCP fingerprinting and is disabled by default. Before enabling this capability, please note DHCP fingerprinting may sometimes result in misidentification of vulnerable devices.

Additional Resources

- Forescout Ripple20 blog
- Executive insights blog by Forescout CEO Mike DeCesare
- JSOF blog
- Video: https://www.youtube.com/watch?v=1UYfDP3v57U

FORESCOUT

Forescout Technologies, Inc.
190 W Tasman Dr.
San Jose, CA 95134 USA

Toll-Free (US) 1-866-377-8771
Tel (Intl) +1-408-213-3191
Support +1-708-237-6591

Learn more at Forescout.com