ExtraHop

SECURITY ADVISORY

Ripple20: Vast Exploitation Threat

EXECUTIVE SUMMARY

Knowledge is the fundamental shield in any security campaign. A perfect understanding of every detail of infrastructure, every valuable asset, and every vulnerability at every second is needed to build an impenetrable defense, with every potential door shut tight and locked. But, it's an imperfect world.

The Ripple20 series of vulnerabilities highlights how modern complexity makes the aspirational goal of an impenetrable defense a Herculean effort. Vulnerable code has rippled outward into hundreds of millions of devices with no obvious connection to the responsible party—the Treck, Inc. library—and no clear sign that the flaw lies hidden in their software.

This report analyzes the extent to which Ripple20 affects businesses around the globe. Using anonymized data from the more than 15 million devices and workloads, ExtraHop has determined that 35 perent of all environments are vulnerable. We will explain this finding and offer guidance on how to approach mitigation of this threat.

INTRODUCTION

Ripple20 is a series of 19 vulnerabilities found in devices that contain the Treck networking stack, a low-level TCP/IP software library developed by Treck that is used in many industries including utilities, healthcare, government, academia, etc., and across a plethora of device manufacturers. The vulnerabilities were announced in June 2020 by the threat research team at JSOF, a cybersecurity research consultancy. Prior to the announcement, the JSOF team spearheading the Ripple20 threat research provided Treck and their vendors an extended 120-day disclosure period to release a patch before the vulnerabilities were made public.

As Treck attempted to track down the vendors affected, it became clear that the complexity of the software supply chains made it exceedingly difficult to know which devices were exposed. Now that the disclosure has been made public, proof-of-concept exploits (POCs) will be created, and we believe companies will begin to see an accelerated exploitation of these vulnerabilities, now and for some time to come. The impact of this threat "ripples" through the complex supply chain, making this a long road ahead for companies working to mitigate this Ripple20 vulnerability.

TABLE OF CONTENTS

EXTRAHOP FINDINGS

ExtraHop analyzes more than four petabytes of anonymized data collected from over 15 million devices and workloads each day across cloud, data center, and remote site deployments. The findings in this report are derived from ExtraHop's data intelligence.

ExtraHop has determined that exposed Ripple20 devices exist in 35% of environments.

> To put this data in context, a typical ExtraHop customer has several Reveal(x) sensors deployed. Some large enterprises have many dozens of sensors deployed to monitor traffic in multiple datacenters, remote sites, and cloud environments. ExtraHop Reveal(x) automatically discovers every device, including IoT, across the network, passively and without agents. Placing sensors across the network provides the best, most complete view of what's happening on the network.

1 in 3 environments are affected by Ripple20

During the JSOF presentation at the 2020 Black Hat Conference, the research team estimated that nearly every business would be affected by the Treck vulnerabilities.

Exposed devices exist in one of three environments monitored by Reveal(x). However, some customers choose not to monitor campus or IoT networks, so we believe 35 percent to be a lower bound on the organizations who are affected.

About the Treck Networking Stack

The Treck network stack has been in use in embedded devices for more than twenty years. Hundreds of millions of devices in the industrial controls, networking, transportation, retail, oil and gas, medical, and other fields that use the Treck software are now known to be vulnerable to exploits. Those exploits can enable attackers to steal data or even execute code.

Identifying vulnerable devices in your environment can be difficult due to the widespread use of the Treck network stack in the firmware of devices such as printers, backup batteries, industrial controllers, and more. While patches have been issued by Treck for all 19 vulnerabilities, due to the age and nature of these devices, patching may prove difficult or impossible.

The difficulties managing these devices combined with the ease with which these devices can be exploited has led our Threat Research team to predict long dwell times if a device is compromised.
Some common devices using the Treck networking stack include:

- HP printers
- Ricoh printers
- Schneider/APC UPS devices
- Digi network tools

For a list of devices known to be vulnerable please see the vendor section of the JSOF release

21% of Ripple20 vulnerabilities have a CVSS score **OVER 9.1**

Critical Vulnerabilities

Of the 19 vulnerabilities, four have a CVSSv3 (Common Vulnerability Scoring System) score of 9.1 or greater. Of these four vulnerabilities that have public details available, CVE-2020-11896 and CVE-2020-11901 allow attackers remote code execution on the vulnerable device. These critical vulnerabilities provide an avenue for attackers to leverage and gain access to the network and maintain persistence in target environments. Given the difficulty administrators will have patching and securing many of the afflicted devices, the likelihood of attackers leveraging these vulnerabilities is high. Additionally, due to the nature of the connected devices, it is near impossible for more traditional security layers, like endpoint detection and response (EDR) or next generation firewalls (NGFW), to prevent exploitation. For more information on these complications please see Identifying Vulnerable Devices.

CVE-2020-11897

CVE-2020-11897 has a CVSSv3 score of 10. This vulnerability is less likely than the others to be exploited because the vulnerability exists in the IPv6 protocol rather than the more traditional IPv4 protocol. As more companies transition from more traditional network protocols, IPv6 usage is on the rise but is currently used in only a small fraction of business networks.

CVE-2020-11896 and CVE-2020-11898

CVE-2020-11896 and CVE-2020-11898 exist because the Treck networking stack improperly handles IPv4 fragments over an IP-in-IP tunnel, allowing attackers remote code execution capabilities. Both CVE-2020-11898 and CVE-2020-11896 stem from the same truncation, shown below.

```
movzx   eax, [ebp+TotalLen]
mov     ecx, [ebp+a0_tsPacket]
cmp     eax, [ecx+tsPacket.pktUserStruct.pktuChainDataLength]
ja      loc_454B30
```

```
movzx   edx, [ebp+TotalLen]
mov     eax, [ebp+a0_tsPacket]
cmp     edx, [eax+tsPacket.pktUserStruct.pktuChainDataLength]
jz      short loc_454181
```

```
movzx   ecx, [ebp+TotalLen] ; CVE-2020-11896
mov     edx, [ebp+a0_tsPacket]
mov     [edx+tsPacket.pktUserStruct.pktuChainDataLength], ecx
movzx   eax, [ebp+TotalLen]
mov     ecx, [ebp+a0_tsPacket]
mov     [ecx+tsPacket.pktUserStruct.pktuLinkDataLength], eax
```

Source: ExtraHop

An encapsulated UDP packet leads to a flow wherein exploitation of CVE-2020-11896 can be achieved. The software concatenates the contents of each fragment into an allocated buffer of the truncated size. The size discrepancy can be abused for a heap overflow.

Furthermore, rather than a truncation, a packet can be crafted that says it is longer than it actually is. If the encapsulated packet is an invalid protocol or otherwise one that is not supported, an ICMP error message responds with heap contents that were adjacent to the sent packet—the information leak described by CVE-2020-11898.

If the CVE-2020-11898 information leak wasn't bad enough, the remote code execution provided by exploitation of CVE-2020-11896 allows an attacker to reliably execute arbitrary code in a device running the Treck networking stack. This gives it the maximum possible CVSS score of 10.0.

Attackers can take over a device through DNS poisoning

CVE-2020-11901

CVE-2020-11901 is a DNS vulnerability which allows attackers remote code execution capabilities via a single invalid DNS response. Due to the ease of exploitation, the ExtraHop Threat Research team believes this vulnerability will be widely exploited and strongly urge security teams to take steps immediately to mitigate the threat (see below for recommendations).

Here's what the Threat Research team at JSOF had to say about the CVE-2020-11901 vulnerability:

> *"In our opinion this is the most severe of the vulnerabilities despite having a CVSS score of 9.0, due to the fact that DNS requests may leave the network in which the device is located, and a sophisticated attacker may be able to use this vulnerability to take over a device from outside the network through DNS cache poisoning, or other methods."* *JSOF, June 2020*

IDENTIFYING VULNERABLE DEVICES

JSOF has stated they expect to expand their research to identify vulnerable devices. As we wait for an expanded list, it is going to be difficult to know all of the affected devices to understand the true impact of Ripple20. There are a few reasons for the difficulty:

- Vendors who embed third party code don't release information on sub-licensed products
- IoT devices aren't typically monitored or catalogued within the context of the rest of the network
- Because of the liberal use of Treck's software, including repurposing and reuse of the code, tracing the supply chain is extremely difficult
- Given the age of the majority of these devices, it's a real possibility the company who developed them may not still be in business making it impossible to track

So what can an organization do to mitigate the effects of the vulnerability? It is critical to determine the likelihood that you will be affected by Ripple20, so the first step is a comprehensive inventory of every device active on the network to determine if any are known to be vulnerable. The next is to understand what the behavior of each device should be and how they interact with other devices and services to understand if there is malicious use. More on mitigation below.

Not a Good Year for VoIP Phones

With the recently disclosed Ripple20 vulnerabilities affecting these devices, the bad news continues for VoIP phones—one of the top device groups to use the Treck networking stack.

Earlier this year, ExtraHop published a security report which looked at the ExtraHop database to determine which devices were connecting to the network during COVID-19, as compared to a baseline measurement pre-pandemic.

Vulnerabilities could be present in your most ubiquitous devices

ExtraHop observed just a 7.5 percent decline in VoIP phones connected to the network during March. This means that, although people aren't in the workplace, relatively few office IP phones have been disconnected. Now, many of those unattended phones remain as possible vectors of attack via Ripple20 and pre-existing vulnerabilities.

And Your Little Printer, Too!

According to ExtraHop's security report on connected devices, VoIP phones weren't the only devices left online when employees left the office. According to the data observed, the vast majority of enterprise printers remained on and connected to the network, with connections between November and March declining by just 0.53 percent.

Printers have long been a target for hackers, and for good reason. According to a 2019 study by NCC Group, there were 49 vulnerabilities uncovered in the drivers and software running on the top six enterprise printer brands. With Ripple20, this number is now even higher.

The challenge here is twofold. First, empty offices mean there may be no one around to disconnect these devices. Second, many of these devices are not just out of sight, but out of mind. Few organizations have a complete device inventory and it's likely that the Ripple20 vulnerability will persist on forgotten devices even when offices reopen.

IMPACT ON IOT DEVICES

What Ripple20 Means for Enterprise IoT Devices

While one may assume that the shift to remote work would help mitigate the risk brought on by the Ripple20 vulnerabilities, the recent security report from ExtraHop revealed that many internet-connected devices remained online and communicating over the corporate network. It is possible that these devices contain the Ripple20 vulnerabilities.

A Difficult Diagnosis for Healthcare

Healthcare organizations often run equipment with embedded software that is difficult if not impossible to update, such as the Ripple20-vulnerable Baxter infusion pumps and certain Carestream products. In cases where updates are possible, it is often difficult to slideline potentially life-saving equipment to perform security updates. As a result, medical facilities need to implement strict security controls, such as connecting Carestream devices to a PC instead of directly to the network.

Even with security practices in place to mitigate the effects of a threat, it can be difficult to implement widespread security controls given the wide variety and large quantity of medical IoT devices in use.

Most impacted devices cannot support agents or logging

JSOF continues to update their list of impacted vendors, found under the vendors section of the release.

Impervious to Endpoint Protection

Many of the devices using the Treck networking stack are running embedded firmware rather than standard operating systems. As such, these devices are not capable of running standard endpoint security agents. Logging, if available, will be limited. Security teams will need to focus on network data to identify and monitor devices. Network or wire data, combined with machine learning can detect compromised devices as well as attempts to exploit vulnerable devices.

MITIGATION

Organizations can take a number of steps to mitigate the risk from Ripple20. Some of these actions will be highly effective but difficult to implement—such as we described above in gaining visibility and applying software patches to all affected devices—while others are good compensating controls, meaning that they will minimize but not eliminate risk.

Patching

JSOF's due diligence in identifying and notifying affected vendors provided them 120 days before the disclosure to produce a patch. However the complicated Treck software supply chain has made it difficult to account for all devices that are using the vulnerable software. Some vendors (not to mention their customers) may not be aware that they are using Treck software—meaning some vulnerable devices will fly under the radar of any patch regime.

Removal From Service

If patching is unavailable, remove devices from service.

If a patch is unavailable for the affected device, ExtraHop recommends that organizations consider removing devices from service entirely and replacing them with secure devices. Removing the device will improve hygiene and compliance, critical for keeping environments secure. Many of the devices affected by Ripple20 vulnerabilities are inexpensive—especially relative to the risk they pose—and may be aging out in any case.

Monitor for Scanning Activity

Before a vulnerable device can be compromised, attackers must first find it. As a best practice, organizations should be scanning their networks to ensure they are not subject to any known vulnerabilities and need to understand which scans are legitimate and which could indicate malicious intent. Attackers have become smarter and will attempt to avoid common detection rules by altering the frequency of the scans, accessing ports out of order, or spoofing their source address. Once attackers find an entry point, they will get inside your network and live off the land to lie in wait until they can escalate privileges to eventually breach the network. Because of the nature of the Ripple20 vulnerabilities, they provide a good hiding place inside the network.

Exploit Detection

Because not all vulnerable devices may be identified and patched, it is crucial that organizations detect attempted Ripple20 exploits as they occur. Network-based detection is a requirement in this case because embedded devices that use the Treck software will not support endpoint agents. As mentioned previously, there are currently no POC exploits for the Ripple20 vulnerabilities, but as a few are relatively easy to exploit (such as CVE-2020-11901), we would expect to see attacks ramp up in the coming months.

Additional Recommended Actions

In circumstances where it is not possible to patch affected devices, it is recommended that you:

- Verify devices are not publicly accessible
- Move devices to a network segment isolated from local subnets
- Drop all IP-in-IP traffic destined for affected devices
- Drop all IPv6 traffic destined for affected devices

Benign vs. Malicious Vulnerability Scanners

Security analysts should pay close attention to the vulnerability scanners running on their networks. While some scanners may be benign and approved by the SOC, analysts should be watching for attackers running similar scans to exploit vulnerabilities.

Dedication to Data Privacy

Data privacy is one of the central challenges of our age. ExtraHop passively monitors every interaction on the network then extracts de-identified metadata to be processed by cloud-based machine learning. So, while we can clearly see how prevalent Ripple20 is across the infrastructures we monitor, we do not link that data to any specific customer. We believe that's the way it should be.