Ripple20: The Threat to Global Software Supply Chains

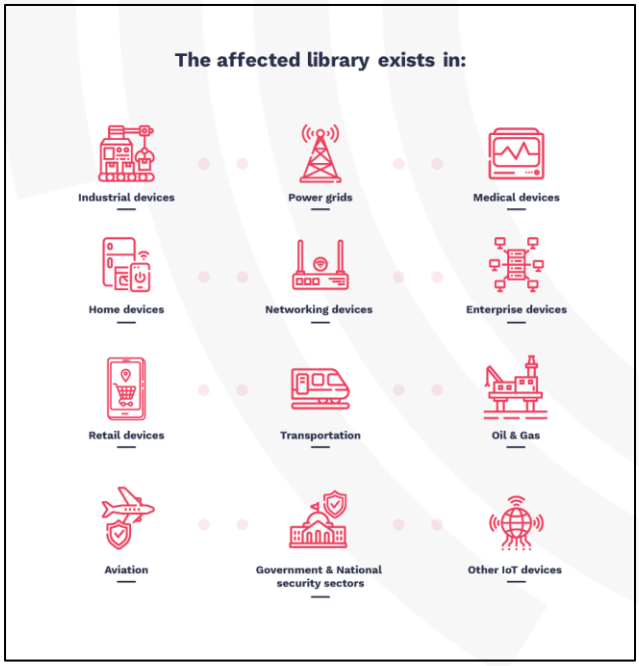
Background

Beginning in September 2019 and announced in mid-June 2020, a team of Israeli security researchers began investigating the code of a little-known Cincinnati-based software company called Treck, Inc. Treck is a leading provider of high-performance TCP/IP solutions for today's embedded applications. These products affect over a dozen industries from industrial devices and power grids to home devices such as printers and IoT-enabled refrigerators.

At the same time, an Israeli company known as JSOF discovered over 19 zero-day vulnerabilities in the networking layer of the TCP/IP protocol which is the backbone of internet-based communications. The team dubbed the group of zero-days **Ripple20**. The JSOF team came up with the name as they realized the magnitude these vulnerabilities will have on the global software supply chain if left unpatched.

These zero-day vulnerabilities allow for remote code execution (RCE). Given that the affected products can be found in the millions operating online, the attack surface for anyone exploiting Ripple20 is enormous.

Affected Industries (spoiler alert, it's all of them)



Affected Vendors

JSOF has provided a listed of identified vendor products that the firm has confirmed through analyzing Treck's code. Vendors have been contacted to identify whether they are impacted by any of the Ripple20 vulnerabilities. The list of those vendors and their status can be found below. In a note from JSOF about patch management of Ripple20, the company had this to say:

> *JSOF has conducted extensive, in-depth analysis, over many months, of the vendors affected by the Treck Internet protocol library vulnerability. The first challenge we experienced was simply being able to identify the relevant vendors! Vendor identity could be obscured through the intricacies of the supply chain. Even when the vendors are identified, patch implementation is complex and not always possible. Over the course of the disclosure process we found that while patching was difficult for some vendors, it could potentially be even more difficult or close to impossible for some end users to install the patches. (For example, if the library is on a separate physical component or the company that produced the component has ceased operations.)*

STATUS: CONFIRMED (8)
B. Braun
Baxter
Caterpillar
HP
Intel
Maxlinear (through HLFN)
Rockwell
Sandia National Labs
Schneider Electric/APC
Digi
HCL Tech

STATUS: NOT AFFECTED (5) (as reported by vendor)
Abbott (through Guidant Healthcare)
Amd
GE Healthcare
Laird
Zebra Technologies

STATUS: PENDING (66)		
Cisco (through Starent)	Hitachi europe	Synamedia(Through Cisco)/NDSUK
EMC (now Dell)	Hlfn	Syncroness
GE general electric (through quadros)	Honeywell	Technicolor (Throught CISCO)
NASA	Itron	Texas Instruments-Berlin
Philips	Kadak	Thinkcom/ThinKom
Verifone	L-3 Chesapeake Sciences Corporation	Tollgrade communications
	Lockheed martin	Ultra Electronics Flightline Systems
**	Maxim Integrated Products	Vicom
Agilent	Memjet	Videotek
Airlinq(throug Netsnapper Technologies SARL)	MTS Technologies	Vocera
Arburg	Netafim	vpacket(now DASAN Zhone)
BAE systems	Netsnapper Technologies SARL	Weibel weibel.dk
BD	NVIDIA (through portalplayer)	Western geco
Broadcom	Portalplayer	Xilinx
Capsule (through digi)	Qualstar.com	Zodiac Aerospace
DASAN Zhone(through vpacket)	Red lion controls	Quadros
Datamax Corporation	Redcom	BECK
Enghouse (through tollgrade communications)	SAIC	KADAK (defuct)
Foundry	ScriptPro	Texas Instruments
Fraunhofer IZFP	Semtech	Marvell
Gainspan (telit)	Sigma Designs	Extreme Networks
Green Hills	SimCom Wireless	Audiocodes
Guidant medical	Starent Networks	

Cybeta

Cybeta Commentary

The challenge with white hat disclosures such as this is that their true intent is as a business development tool, regardless of the usefulness of the research itself. The announcement alerts customers and attackers at the same time and in order to obtain specific details of remediation and products affected, one must contact the research company thereby creating a potentially critical delay in proper response. At the same time, the threat actors are aware of large swaths of potential targets. Once exploits are developed and/or become available to the broader attacker market, you have the perfect storm for mass exploitation. Although CISA and the research groups often have pre-communicated with critical industries prior to disclosure, this leaves large pockets both domestically and globally of newly informed and therefore inadequately protected corporations.

Treck has reportedly remediated a large portion of affected underlying code. The challenge now will be in making sure that all devices in a company's registry are accurately catalogued so that the expedited patch management comprehensively covers all connected devices. In addition, RIPPLE20 will continue to result in new identified vulnerabilities and affected devices creating a perfect storm of critical patches with diverse products in a company's supply chain.

Suggested Remediation Steps

Although an imperfect process due to the disclosure pattern used by JSOF, in order to best mitigate the above conditions Cybeta suggests following the below protocol:

Priority 1:

1. Review the above confirmed or potentially affected vendors
2. Refer to or complete an inventory of the externally visible technologies to obtain exact version/patch/upgrade data
3. For any externally visible technologies that match the affected vendors, confirm the latest patches are applied
4. Prioritize each potentially affected technology by criticality to business continuity
5. Contact vendors directly to determine if latest patches address **CVE-2020-11896/97/98/99**
6. For all technologies that are unable to be patched, implement mitigating controls such as those found below to remove their access to external connections via TCP/IP

Priority 2:

1. Review above confirmed or potentially affected vendors against an internal asset inventory
2. Prioritize each potentially affected technology by criticality to business continuity
3. Confirm that the latest patches are applied
4. Contact vendors directly to determine if their latest patches address **CVE-2020-11896 and CVE-2020-11898**
5. For all technologies that are unable to be patched, implement mitigating controls to remove their access to external connections via TCP/IP

Priority 3:

1. Review vendor/supply-chain partners
2. Prioritize each vendor by criticality to business continuity starting with those with direction connections into your network
3. Contact vendor partners to verify mitigation status
4. For all vendors with access, criticality and potential vulnerability but who are not yet remediating the vulnerability, consider additional mitigating controls such as suspending direct network connections or placing connections in a compartmentalized and monitored network segment
5. For all vendors who confirm mitigation is in place, work with your threat intelligence team or vendor to verify adequacy

CERT CC Manual Mitigation Suggestions
https://github.com/CERTCC/PoC-Exploits/blob/master/vu-257161/recommendations.md

1. CVE-2020-11896 and CVE-2020-11907 can be mitigated by inspection of IP fragments and rejection of anomalous IP fragment traffic to prevent abuse. If IP fragmenting is not supported, you may also block IP fragmented packets entirely as a protective precaution.
2. CVE-2020-11897 and CVE-2020-11909 can be mitigated by blocking various IP source routing, including IPv6 source routing - Routing Header Type 0 that has been deprecated by RFC-5095, see also (VU#267289)[https://www.kb.cert.org/vuls/id/267289]
3. CVE-2020-11898, CVE-202-11900 and CVE-2020-11902 can be mitigated by disabling or blocking IP-in-IP tunneling if is not supported or required in your environment. More information can be found here VU#636397
4. CVE-2020-11899 can be mitigated by dropping IPv6 pcakets addressed to multicast destination ff00::/8
5. CVE-2020-11901 can be mitigated by normalizing DNS responses through DNS deep packet inspection or by a secure DNS recursion server.
6. CVE-2020-11903 and CVE-2020-11905 can be mitigated by disabling DHCP and DHCPv6 clients, ensuring the DHCP Relay option (RFC3046)[https://tools.ietf.org/html/rfc3046] is not enabled, and the local area network switch has capabilities such as DHCP-snooping to reduce risk of DHCP abuse on the target device.
7. CVE-2020-11910 and CVE-2020-11911 can be mitigated by blocking unsupported ICMP messages such as ICMPv4 type 3, code 4, packets (MTU update) and ICMP type 18 code 0, packets (Address Mask Reply). These messages are not required in most end device network environments.
8. CVE-2020-11913 and CVE-2020-11914 can be mitigated by ensuring use of reliable Ethernet hardware that rejects runt frames uses proper device driver protections to reject malformed Ethernet frames.
9. CVE-2020-11912 can be mitigated by a firewall device or NAT device that inspects TCP SACK (Select Acknowledgement) and TCP timestamp options, rejecting any malformed packets.