

Ripple20: How Ordr Can Help Detect And Mitigate These Vulnerabilities

ORDR SECURITY BULLETIN

JUNE 2020

Ripple20 – How Ordr Can Help Detect and Mitigate These Vulnerabilities

Earlier this week, the <u>cybersecurity firm JSOF</u> published information on 19 vulnerabilities that affect many IoT devices. Specifically, JSOF discovered 19 vulnerabilities inside the Treck TCP/IP stack that is used by many device manufacturers and enables their devices to communicate over a network. The vendor list of vulnerable devices includes device manufacturers such as Baxter, Intel, Caterpillar, Cisco, Aruba, HP, and Xerox, that have all issued their own advisories and patches. However, the list of affected devices continues to grow as this vulnerability has been present inside the Treck stack for likely more than 20 years and implemented in thousands of devices since then. Organizations are now scrambling to assess their exposure by identifying any vulnerable assets in their inventory, and then respond by either patching or implementing compensating controls to protect at-risk devices.

Ordr Systems Control Engine (SCE) can

- Identify vulnerable assets impacted by Ripple20
- Detect Ripple20 cyberattacks
- Proactively protect devices from Ripple20 attacks
- Take swift action when a Ripple20 attack is detected

Identifying Devices Vulnerable to Ripple20

Ordr exercises a combination of manufacturer advisories and proactive probing to track devices that are vulnerable to Ripple20. Ordr has curated a list of known vulnerable devices and will compare them to matching inventory in Ordr SCE customer environments automatically through our new Ripple20 feed service. This feed of vulnerable devices will be kept up to date and ensures organizations will be continually apprised for vulnerabilities as soon as the information is made available. Accompanying the Ripple20 feed service are links to the manufacturer's advisory as well as to any patches the vendors have made available to address the Ripple20 vulnerabilities. One major challenge is reliance on vendor identification and disclosure. Because the Ripple20 vulnerabilities have been present for 20 years, the affected device list is growing every day, and there are several major device manufacturers who are researching to see if any of their devices are vulnerable. Therefore, Ordr is also developing novel methods to proactively identify

devices that are using the vulnerable Treck TCP/IP stack both passively and actively on the network. Below is an example of a device in our lab that has been detected using the vulnerable Treck stack.

ōrdr	💵 Dashboard 🥆 Group 🏽 Profile 📮	a Device ⁹ 🕈 Application 🖶 Network 🖿 System					l	a 🖸 😁
Device Menu 🛶 🕂	Device - hq	1.ordr.net (192.168.102.11)						
L Device List	③ Details 常 Security Incidents 器 FI	low Genome 🔟 Network Stats 😆 Known Vulnerabilities						
🖙 Safe Device List 🧶								
🚨 User List	Nac Address : Device Description : Drinter			Classified		Ripple20-test-sensor		
Limited Visibility Endpoints	Manufacturer : Model Name/No -			Proints_bo Printers and foxiers		192.168.102.0/24 VI M0002 (2)		
Ext. Communication	Serial No.: N/A			11111111 1 0162 (02511)				
				IoT Endpoint				
Advance Tasle -	SW Version : Liteck ICP-IP FODN : ha.ord	lenet		451		N/A 6/23/2020 7:39:42 PM		
Advance tools :	DHCP Hostname :							
ες, Data Schema								
🗙 Data eXchange						CN=Preset Certificate		
🗞 Import Asset Info						1/1/2000 12:00:00 AM		
👸 Utilization Schedule								
						Unspecified		
			Click to provide class	ification feedback				
							8	AVE CHANGES
	Concession in which the local division in which the local division is not the local division in the local dint							
		Tags: New Tag +						
		Criticality LEVEL_3						
	List of Devices							
					0	Em Q An		Manage 🕰
	Clear all criteria Devices with Critical Risk $ imes$							

Ripple20 will show up in the Known Vulnerabilities tab for this device:

Device - hq.ordr.net (192.168.102.11)						
🛈 Details 🗳 Secu	rity Incidents 🕱 Flow Genome 🔟 Network Stats 🗯 Known Vulnerabilities		G X			
1 vulnerability						
ID	Description	State	Score			
ICSA-20-168-01	Vulnerabilities: Improper Handling of Length Parameter Inconsistency, Improper Input Validation, Double Free, Out of bounds Read, Integer Overflow or		10.0			

To help guarantee organizations can accurately identify any system vulnerable to Ripple20, whether it has been published or not, Ordr has built a Ripple20 active scanner incorporated into the Ordr SCE product. Ordr worked with the JSOF team to ensure our Ripple20 scans would accurately detect vulnerable versions of the Treck stack utilized by devices. Ordr's Ripple20 scanner dynamically identifies, or verifies, that a device is at risk. The Ripple20 scanner has minimal operational impact, and it can be tuned to only scan specific device types or areas of the network. Below is an example of how customer can initiate vulnerability scan, looking for Ripple20 impacted endpoints.

itical Risk 🗙

ōrdr	🗄 Dashboard I Group 🖷 Profile 🗖 Device 🎱 Application	on 🕀 Network 🖿 System					B 0 0
System Menu	Job - Unsaved Job						
Endinuction	O Details						×
Sector Deservator							
System Parameters	Job Name: Unsaved Job						
dia 215 2612012	Scan Engine:						
Service Integration	Ordr Select Policy V O						
Intranet Ranges	Initiate: System Discovery						
C the Accests	Vulnerabilities Host Discovery scan						
Audit Trail	Include: Urgent/11 Discovery						
	Except: Full and very deep						
	Parts to include:						
							Save
	Scanning Jobs Browser						
	Scalining 5005 browser						×
					Q. Any Visible Fiel		Manage ED, 💼
	No. Job Name		Scan Engine	🗧 Last Run Status	C Schedule	Actions	
	1 Ripple20 test1	Vulnerabilities	Ordr	Completed at 6/24/2020, 12:29:12 AM	On 6/24/2020 @0.29 AM	1 E0	
-		-					
orar	E Dashboard 🕆 Group 🔍 Profile 📮 Device 🏾 🏵 Application	Network System					
Device Menu 🖃	Device - hq.ordr.net (192.16	58.102.11)					c and a she in the
⊑o Device List	🛈 Details 📽 Security Incidents 🕱 Flow Genome 🖬 Netwo	rk Stats 🔅 Known Vulnerabilities					G ≡ ×
🖙 Safe Device List 🌘							
🚨 User List	ID Description					State	Score
Limited Visibility							10.0
Endpoints							
Ext. Communication							
Advance Tools :							
🛱 Data Schema							
Y Data aYrbanna							
A new countings							
S Import Asset Info	List of Devices						

 Image: String Comp
 Profile
 O
 Rink
 Wate
 Profile
 <t

RIPPLE20 ORDR SECURITY BULLETIN

When devices are discovered that are vulnerable to Ripple20, either due to the feed service or the active scanner, they are listed inside the Ordr Security Dashboard.

ōrdr	🚦 Dashboard 🐤 Group 🔹 Profile 🗔	Device 🍄 Application ⊕ Network 🖿 System			£ 6
Dashboard Menu →	Incident Summary - Total 197				UTC Daily Statistics : 6/24/2020 12:26:03 PM, in-progress
✤ Executive Summary	Sessions Exporting Data	Open External Channels	External Communications	Internal Communications	Infections & Vulnerabilities
Incident Summary & Device Risk Summary	۵۵ ک	۰ ې 🕑	<u>•</u> 1	91 📭	. 105 ↔
Fill Inventory Dusbboard	™⊇ Bytes Total	≡ 0 (£C	№? 1 Unwanted URL ● O Susp. Domain ● O Blacklist IP ◆ O Phishing № O Bad URL ® O Inappr. Content △ O Mining	Image: Space of the second	 62 Miss. Infection 28 Known Vuln. 10 Cert Expiry 3 VxWorks IPnet 2 Ripple20 Vuln. 0 Session Vuln. 0 SW Vuln. 0 PWD Vuln.
	Incidents of Data Exciltration	Incidents of Opened External Channels	Incidents of Abnormal External Communication	Incidents of Abnormal Internal Communication	Incidents of Device Infection or Vulnerability
	Device Risk Summary				
	Critical Risk 💷 📼	High Risk 📧 📼	Medium Risk 💼 📼	Low Risk 😐 📼 📼	Normal 📧 📼
	2	24	40	12	664
	Devices with Risk Score of 9.0 and above Count for today so far	Devices with Risk Score of 7.0 to 8.9 Count for today so far	Devices with Risk Score of 4.0 to 6.9 Count for today so for	Devices with Risk Score of 0.1 to 3.9 Count for today so far	Devices with Risk Score of 0 Count for today so far

Here is an example of a vulnerable device, and more detailed information about the CVE detected.

ōrdr	🚦 Dashboard 😚 Group 🐞 Profile 🗖	🗅 Device 🥙 🍄 Application 🕀 Network 🗈 🗈	iystem				B 🖸 😁			
Device Menu 🖃	Device - hc	1.ordr.net (192.168.102.11)								
L o Device List	🛈 Details 🏾 📽 Security Incidents 🗶 F	low Genome 🔟 Network Stats 🗯 Know								
Safe Device List	Notes / Note / Security Notes for Not V2/2020 10:00/M									
≜ llserlist										
Limited Visibility							•			
S Lot Communication							•			
CAL CAMMARCANAN					Security Incident	Density Shades for the 4-Hour Internal occurance counts below:	2 3 4 5 6 7 8 9 10 way			
	 Ripple20 Vulnerabilities : Incident Score(10.0) - 	Ripple20:(from Scan) Treck TCP Stack multiple vulnerabiliti	rs : Peer (); happened once							
Advance loois :	🔹 Rapison Attack Rapis on Marcis : Incident Source(2-0): DMP4 parameter problem with turnel incide: Peer (192:168:10:211); Ocument (300 incide)									
C Loco Literia Data eXchange S Import Asset Info Utilization Schedule	Let Ourneye 673/2000 92:64 PN [Stroll down to see all ocurrences] Decription DPV+ parameter problem with turnel inside in Amenduan Ourneys 62/37/2000 92:54 RM bite 62/37/2000 92:54 RM bite 67/37/2000 92:54 RM									
	Ripple20 Attack : Ripple 20 Attacks : Incident Sci	ore(2.0) - anomalous ICMPv4 type 3,code 4 Path MTU Disco	very : Peer (192.168.102.11); Occurred 200 times							
	 Ripple20 Attack : Ripple 20 Attacks : Incident Sci 	ore(2.0) - anomalous ICMPv4 Address Mask Reply message	(type 18, code 0) : Peer (192.168.102.11); Occurred 100 times							
	List of Devices									
	Total 2 Devices match 1 filter 💿 🙉 🗛 violabe Total 😑 con investment schöring turnents.									
	C Creation Review = Michica Rek X									
	↓ I						🖆 🚊 🛨 Classification View 🗸			
	No. Mac Address O IP Address O	Device Name	C Group) Profile	C Risk V	uln () Info			
	2 192 108 102 12	ba orde net	Printers and Copiers							

A report can also be generated for auditing or reporting purposes from Ordr SCE.

Please note that Ordr SCE seamlessly integrates with external vulnerability assessment tools such as Tenable and Rapid7. Organizations using those tools to detect devices vulnerable to Ripple20 can integrate them into the Ordr SCE inventory and security dashboard. Additionally, Ordr can also transmit lists of vulnerable devices and device types back to external vulnerability assessment tools for a more aggressive scan, if wide scanning is not an option or if some devices will not react kindly to an aggressive scan.

Detect Active Exploitation of Ripple20

Ordr SCE has a built-in Network Intrusion Detection System (NIDS) engine which monitors traffic traveling throughout the network. Our NIDS rules have been updated to detect the Ripple20 vulnerability behavior. This is a distinct advantage over reliance on traditional firewalls that typically only monitor traffic coming through north-south, perimeter ingress/egress on the Internet edge. In order to exploit most of the Ripple20 vulnerabilities, attackers need to be on the same segment or in the same VLAN, rendering traditional perimeter-based firewall solutions ineffective. Ordr SCE monitors every device communication passively and checks against our NIDS rules. This generates instant alarms against devices that are being exploited, along with the attack vectors, such as devices that initiated attack, complete visibility of the attacking device, and retrospective record of communications during attack.

There are many NIDS CVEs that correspond to active Ripple20 attacks, as shown in the following table, and they are all included in the Ordr NIDS engine.

CVEs	CVSSv3	Details
CVE-2020-11896	10	Remote Code Execution by sending multiple malformed IPv4
		packets to a device supporting IPv4 tunneling.
CVE-2020-11897	10	Out-of-Bounds Write by sending multiple malformed IPv6
		packets to a device.
CVE-2020-11901	9	Remote Code Execution by answering a single DNS request
		made from the device. This affects any device running the Treck
		TCP/IP stack with DNS support.
CVE-2020-11898	9.1	Improper handling of the Length Parameter Inconsistency in
		IPv4/ICMPv4 component.
CVE-2020-11900	8.2	Possible Double Free in IPv4 tunneling component
CVE-2020-11902	7.3	Improper Input Validation in IPV6OverIPv4 tunneling component

CVE-2020-11904	5.6	Possible Integer Overflow or Wraparound in Memory Allocation
		component
CVE-2020-11899	5.4	Improper Input Validation in IPv6 component
CVE-2020-11903	5.3	Possible Out-of-Bounds Read in DHCP component
CVE-2020-11905	5.3	Possible Out-of-Bounds Read in DHCPv6 component
CVE-2020-11906	5	Improper Input Validation in Ethernet link layer component
CVE-2020-11907	5	Improper Handling of Length Parameter Inconsistency in TCP
		component
CVE-2020-11909	3.7	Improper Input Validation in IPv4 component
CVE-2020-11910	3.7	Improper Input Validation in ICMPv4 component
CVE-2020-11911	3.7	Improper Access Control in ICMPv4 component
CVE-2020-11912	3.7	Improper Input Validation in TCP component
CVE-2020-11913	3.7	Improper Input Validation in IPv6 component
CVE-2020-11914	3.1	Improper Null Termination in DHCP component
CVE-2020-11908	3.1	Improper Null Termination in DHCP component

When an exploit attempt is detected, the security dashboard is updated as shown below, and details of the issue are called out, including aggressor and target of the attack.



Optionally, security incidents can be shared with Security Information and Event Management (SIEM) tools

like Splunk, and workflow orchestration tools like ServiceNow and Nuvolo so they can tie into existing response and remediation processes.

Protect Vulnerable Devices

Organizations should contact their device manufacturer to obtain patches for Ripple20. If you have devices that cannot be patched in a timely fashion, Ordr SCE can implement microsegmentation as a compensating control to limit the surface area of attack while ensuring the device's continued operation.



Safeguards against compromise can be achieved by provisioning security policies with Access Control Lists (ACLs) based on device behaviors observed by Ordr SCE. The policy enforcement can be enabled directly from Ordr SCE and enforced through our integrations with network switches, wireless controllers, and sent to NAC solutions such as Cisco Identity Services Engine (ISE) or HPE Aruba ClearPass, or protected with zone-based security on next-generation firewalls including Palo Alto Networks, Check Point, Fortinet, and Cisco. In the screenshot below are all of the endpoints that a device vulnerable to Ripple20 regularly communicates with; ACLs can be easily deployed to allow/deny connections to specific devices, and networks.

Dev	Device Policy List														
									۹		Any Visible Field	= case insensitive s			
				Allow a Domain	Allow Internal	Remove Selected Entries	Generate CLI	Enforce Policies at Firewall	Enforce Pol at Switc	licies :h	Remove Firewall Enforcement	Remove Switch Enforcement			
≡×	No.	Туре	Scope	Peer IP / Domain						Peer IP N	lask	Protocol	Dst Port	Action	
			Profile												
Dev	vice	Flow List													

In the case of Ripple20, Ordr SCE can automatically generate appropriate ACLs allowing the required communications and denying unnecessary access to devices that are vulnerable to Ripple20. This process is typically the most time-consuming part of an organization's security as it takes multiple efforts to combine device visibility and device behavior to build right security policies. Ordr automates this.

Take swift action

In cases where Ordr SCE sees suspicious activities from potentially compromised endpoints, the Ordr SCE operator can immediately initiate the remediation process by sending appropriate policy change to the network switches, connection infrastructure, or firewalls to isolate and quarantine offending devices. Sample

remediations may include the use of enforcing quarantine Virtual LANs (VLANs) or denying network access to the compromised endpoint completely through blacklisting and/or shutting down the compromised endpoint's network port. This can be performed directly from Ordr SCE through our integrations or automated through NAC tools like Cisco ISE and HPE Aruba ClearPass.

List of Devices									
Total 2 Devices match 1 filter 🔊 🖪 🔍 Any Visible Field = case insensitive substring to match Manage 🕰									
𝕂 Clear all criteria Devices with Critical Risk ×	V. Clearal criteria Devices with Critical Risk ×								
◆ 王				🖆 🖳 🛧 Classification View 🗸					
Add to Blacklist (1 Row) Blacklist (1 Row) Blacklist (1 Row) Blacklist (0 Rows)	Remove Blacklist & Enable Ports (0 Rows)	Fetch Installed Software Info (1 Row)	(1) Row)	O Analyze Attributes App Usage (1 Row) (1 Row)					
Ev No. Mac Address 🔅 IP Address 🔅 Device Name	🗘 Group	🔅 Profile	🗘 Risk 🔿	Vuln 🔅 Info					
1 192.168.102.12				critical 🈩 🛣 🕼 🍄 👙					
2 2 192.168.102.11 192.168.102.11				critical 🈩 🛣 📠 👼 🏶 👙					

Conclusion

Ripple20 vulnerabilities reinforce the challenges organizations face with connected IoT and OT devices. These threats also validate the need for proactive protection based on rich visibility of connected devices and their behavior to combat vulnerabilities like Ripple20 and for other vulnerabilities that are right around the corner.

Please contact the Ordr team for a demo and discussion on how to protect your assets from the neverending vulnerability advisories.

take control.

info@ordr.net www.ordr.net

2445 Augustine Drive Suite 601 Santa Clara, CA 95054