Ripple20: How Ordr Can Help Detect And Mitigate These Vulnerabilities

ORDR SECURITY BULLETIN

Ripple20 – How Ordr Can Help Detect and Mitigate These Vulnerabilities

Earlier this week, the cybersecurity firm JSOF 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.

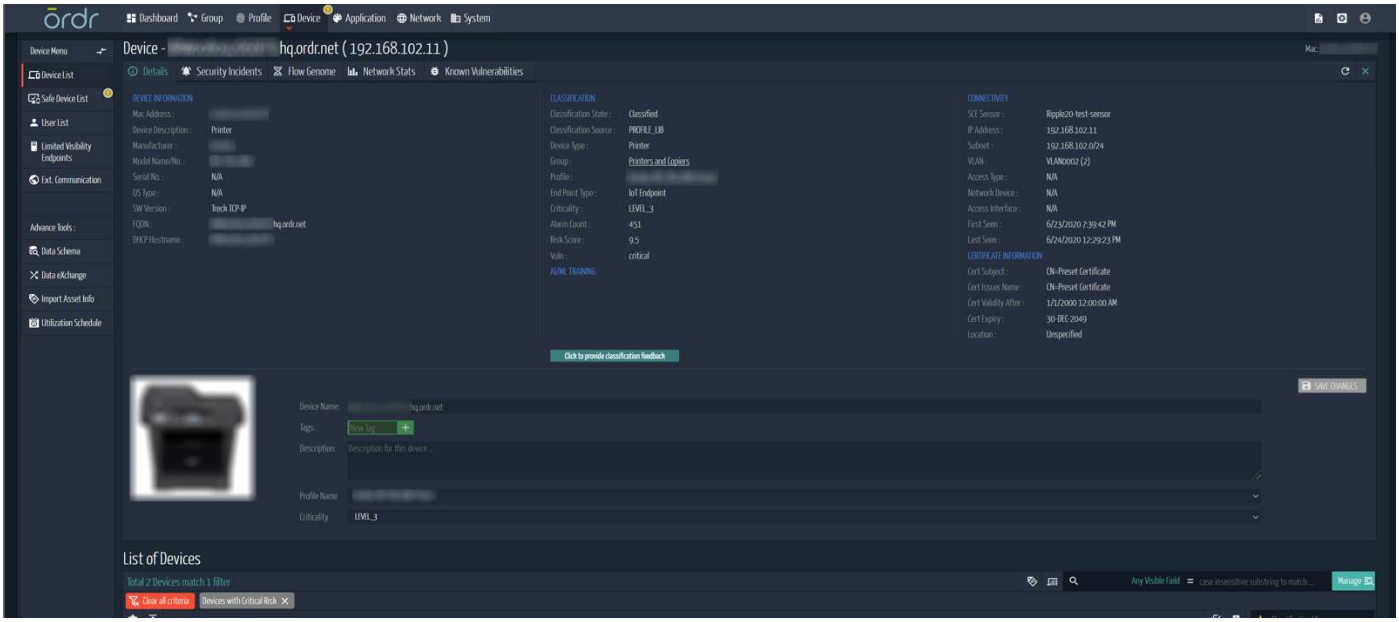
Ordr Systems Control Engine (SCE) can

- 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

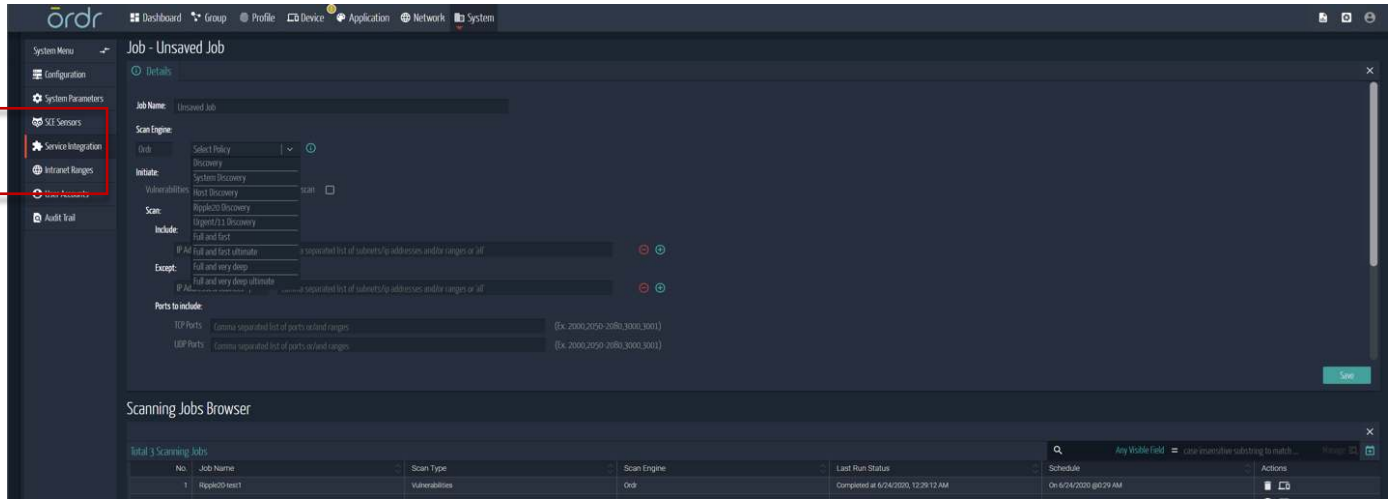
Ordr exercises a combination of manufacturer advisories and proactive probing to track devices that are vulnerable to Ripple20. Ordr has curated a list of known vulnerable devices and will compare them to matching inventory in Ordr SCE customer environments automatically through our new Ripple20 feed 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

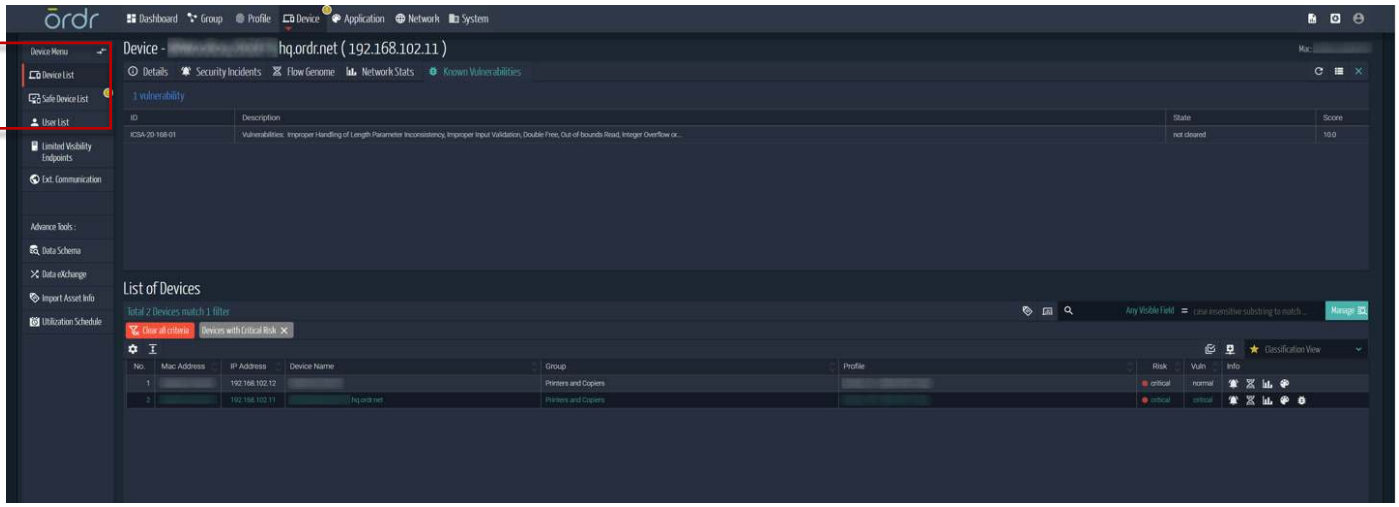
devices that are using the vulnerable Treck TCP/IP stack both passively and actively on the network. Below is an example of a device in our lab that has been detected using the vulnerable Treck stack.



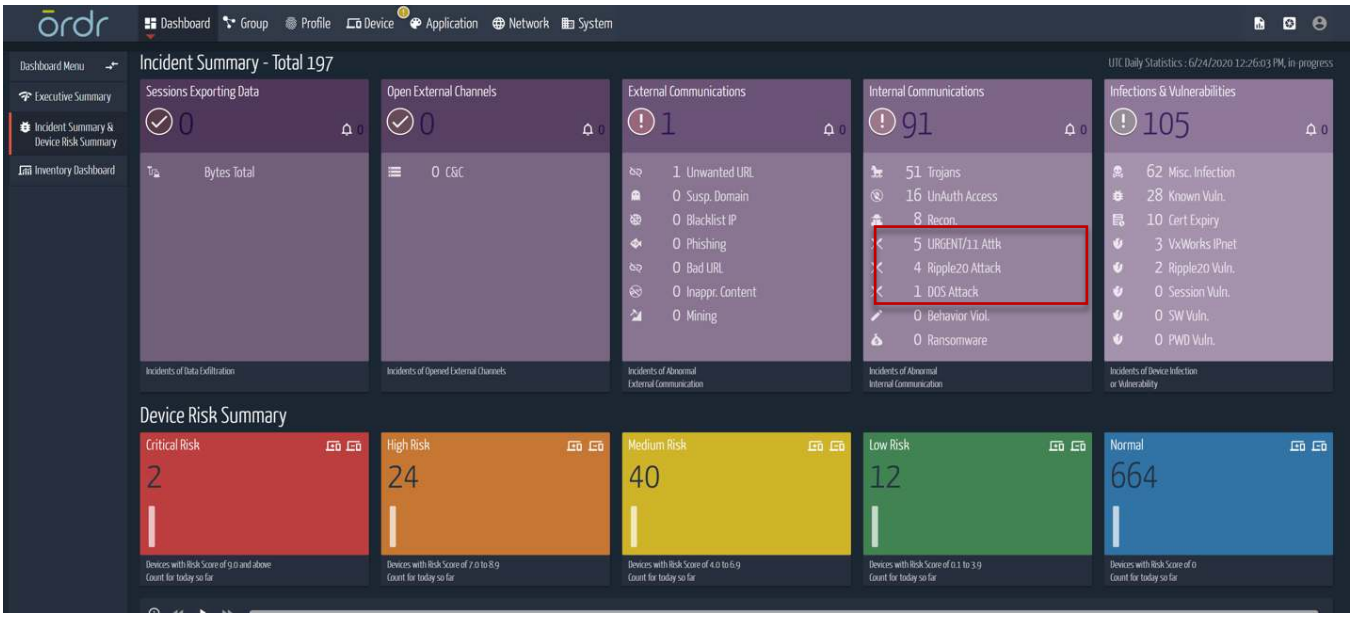
Ripple20 will show up in the Known Vulnerabilities tab for this device:

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.

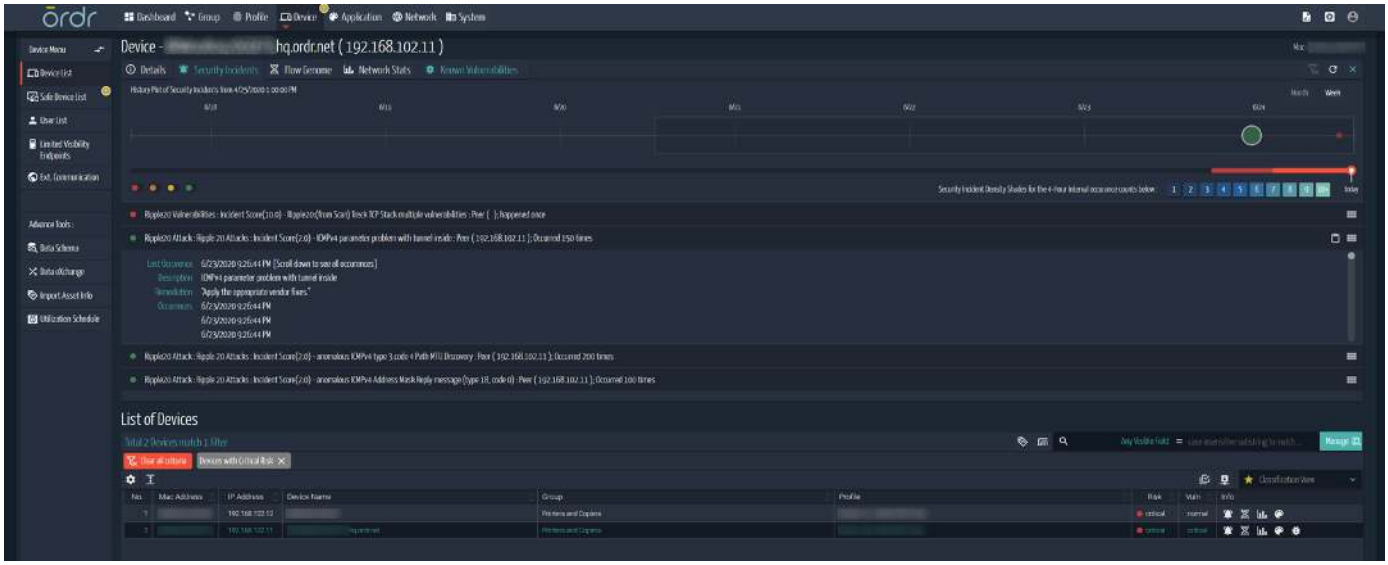

ordr
Dashboard
Group
Profile
Device
Application
Network
System
System Menu
Configuration
System Parameters
SCE Sensors
Service Integration
Intranet Ranges
Audit Trail
Job - Unsaved Job
Details
Job Name:
Unsaved Job
Scan Engine:
Initiate:
Scan:
Include:
Except:
Ports to include:
TCP Ports
UDP Ports
Save
Scanning Jobs Browser
Total 3 Scanning Jobs
No.
Job Name
Scan Type
Scan Engine
Last Run Status
Schedule
Actions


ordr
Dashboard
Group
Profile
Device
Application
Network
System
Device Menu
Device List
Safe Device List
User List
Limited Visibility Endpoints
Ext. Communication
Advance Tools :
Data Schema
Data eXchange
Import Asset Info
Utilization Schedule
Device - hq.ordr.net (192.168.102.11)
Details
Security Incidents
Flow Genome
Network Stats
Known Vulnerabilities
1 vulnerability
ID
Description
State
Score
ICSA-20-168-01
not cleared
10.0
List of Devices
Total 2 Devices match 1 filter
Clear all criteria
Devices with Critical Risk
No.
Mac Address
IP Address
Device Name
Group
Profile
Risk
Vuln
Info
192.168.102.12
Printers and Copiers
192.168.102.11
hq.ordr.net
Printers and Copiers

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.



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



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

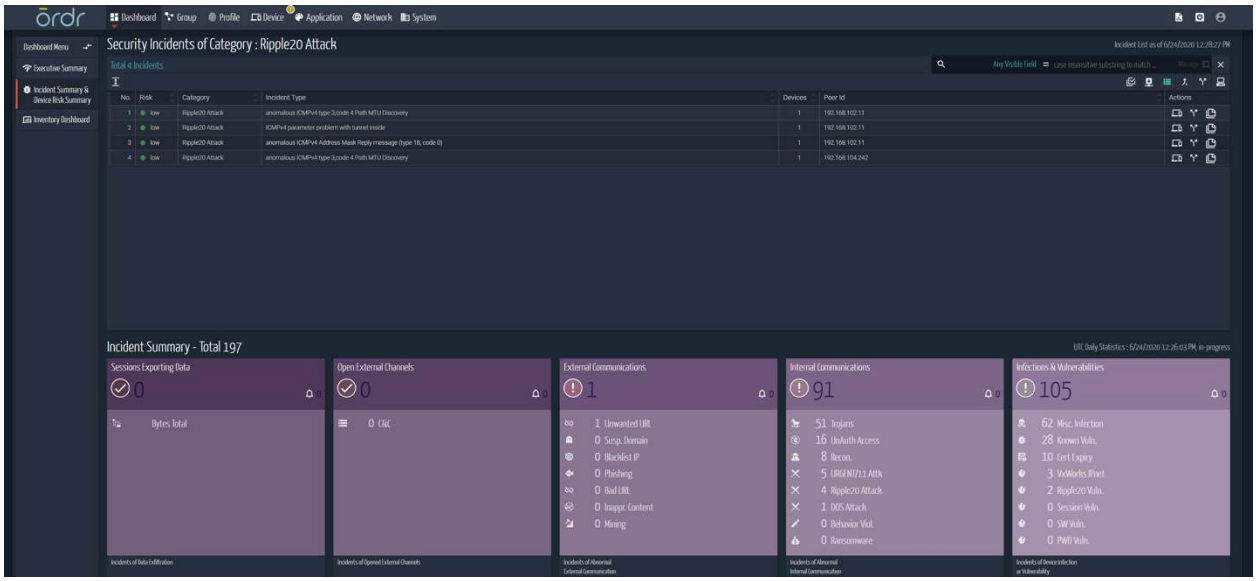
Ordr SCE has a built-in Network Intrusion Detection System (NIDS) engine which monitors traffic traveling throughout the network. Our NIDS rules have been updated to detect the Ripple20 vulnerability behavior. This is a distinct advantage over reliance on traditional firewalls that typically only monitor 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.

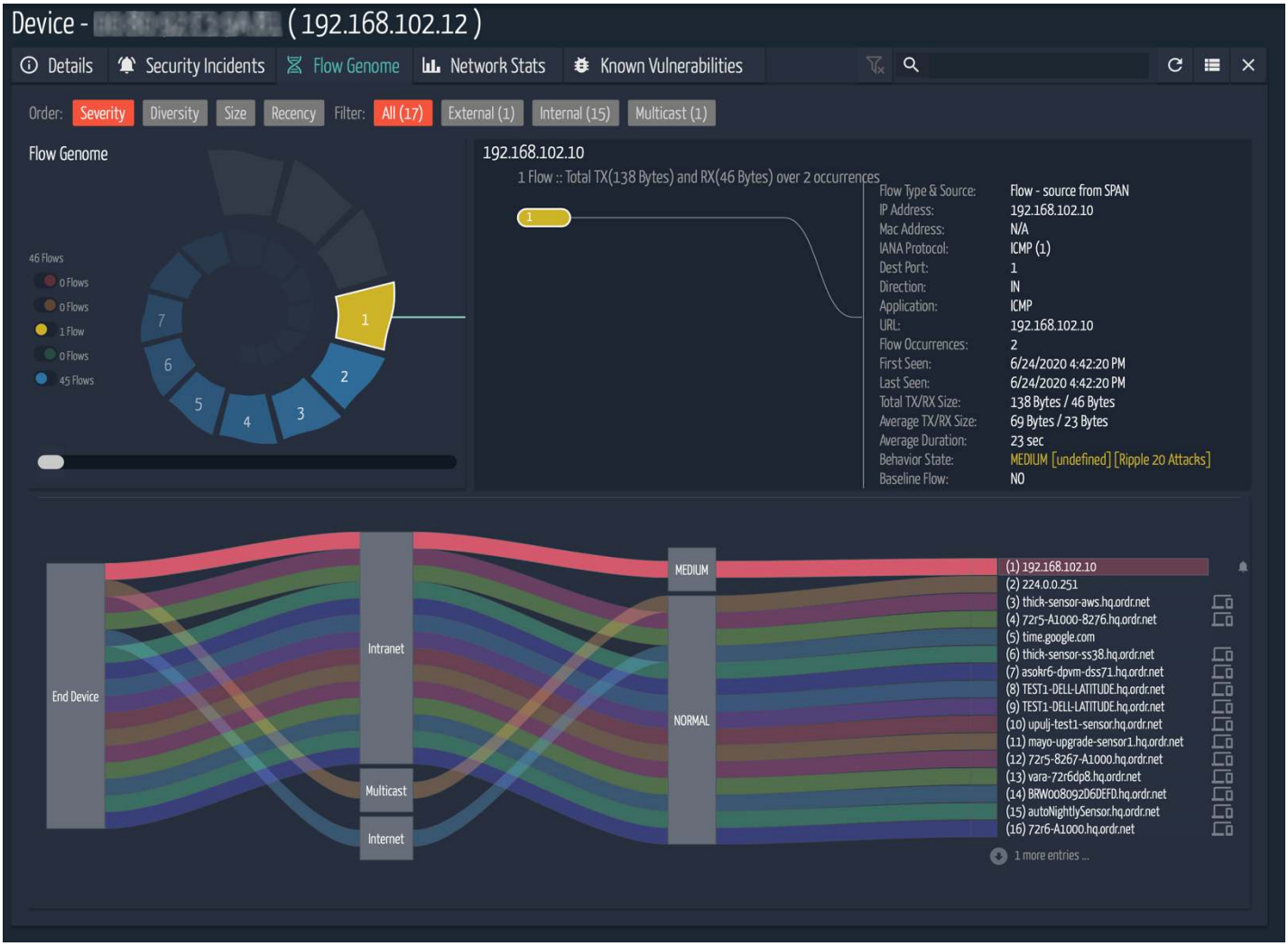


Optionally, security incidents can be shared with Security Information and Event Management (SIEM) tools

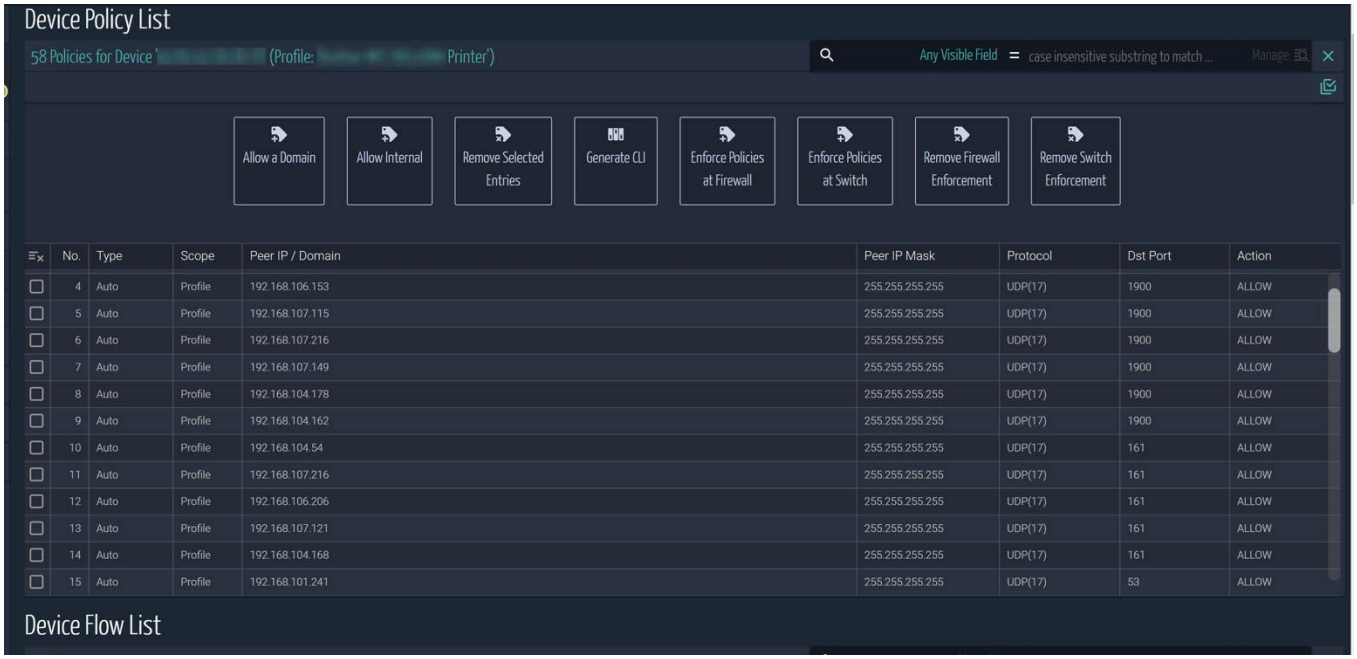
like Splunk, and workflow orchestration tools like ServiceNow and Nuvolo so they can tie into existing response and remediation processes.

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.



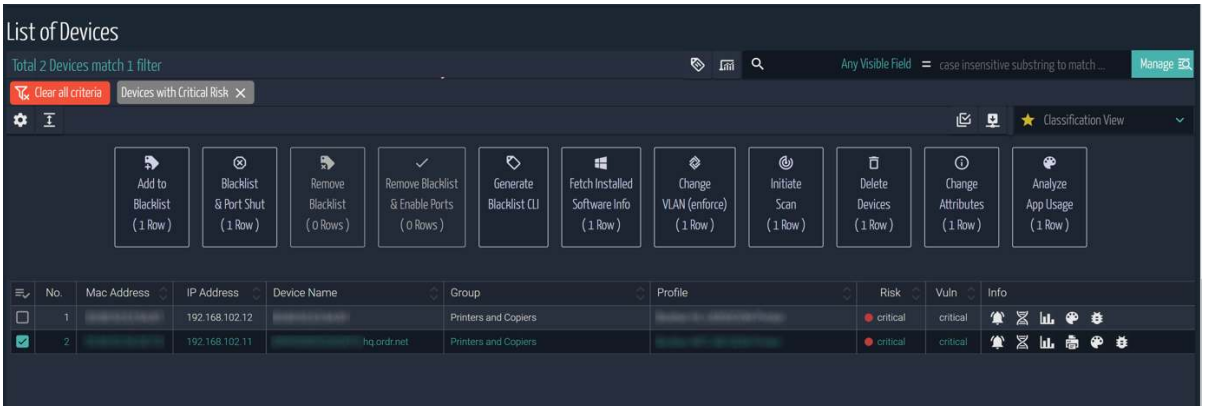
No.	Type	Scope	Peer IP / Domain	Peer IP Mask	Protocol	Dst Port	Action
4	Auto	Profile	192.168.106.153	255.255.255.255	UDP(17)	1900	ALLOW
5	Auto	Profile	192.168.107.115	255.255.255.255	UDP(17)	1900	ALLOW
6	Auto	Profile	192.168.107.216	255.255.255.255	UDP(17)	1900	ALLOW
7	Auto	Profile	192.168.107.149	255.255.255.255	UDP(17)	1900	ALLOW
8	Auto	Profile	192.168.104.178	255.255.255.255	UDP(17)	1900	ALLOW
9	Auto	Profile	192.168.104.162	255.255.255.255	UDP(17)	1900	ALLOW
10	Auto	Profile	192.168.104.54	255.255.255.255	UDP(17)	161	ALLOW
11	Auto	Profile	192.168.107.216	255.255.255.255	UDP(17)	161	ALLOW
12	Auto	Profile	192.168.106.206	255.255.255.255	UDP(17)	161	ALLOW
13	Auto	Profile	192.168.107.121	255.255.255.255	UDP(17)	161	ALLOW
14	Auto	Profile	192.168.104.168	255.255.255.255	UDP(17)	161	ALLOW
15	Auto	Profile	192.168.101.241	255.255.255.255	UDP(17)	53	ALLOW

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.



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 never-ending vulnerability advisories.

info@ordr.net
www.ordr.net

2445 Augustine Drive Suite 601
Santa Clara, CA 95054