VxWorks URGENT/11

How Ordr Protects Your Assets

Two months after a security firm disclosed 11 vulnerabilities (called URGENT/11) found in specific versions of VxWorks (Real Time Operating System) by Wind River, the U.S. Food and Drug Administration (FDA) released its safety communications to the healthcare industries. The FDA warned that the exposure to vulnerabilities in a 3rd party software stack (IPnet) extends beyond VxWorks, but also several other RTOS's. 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, detect URGENT/11 cyberattacks, proactively protect devices from current and future vulnerabilities, as well as take swift action when bad things do happen.

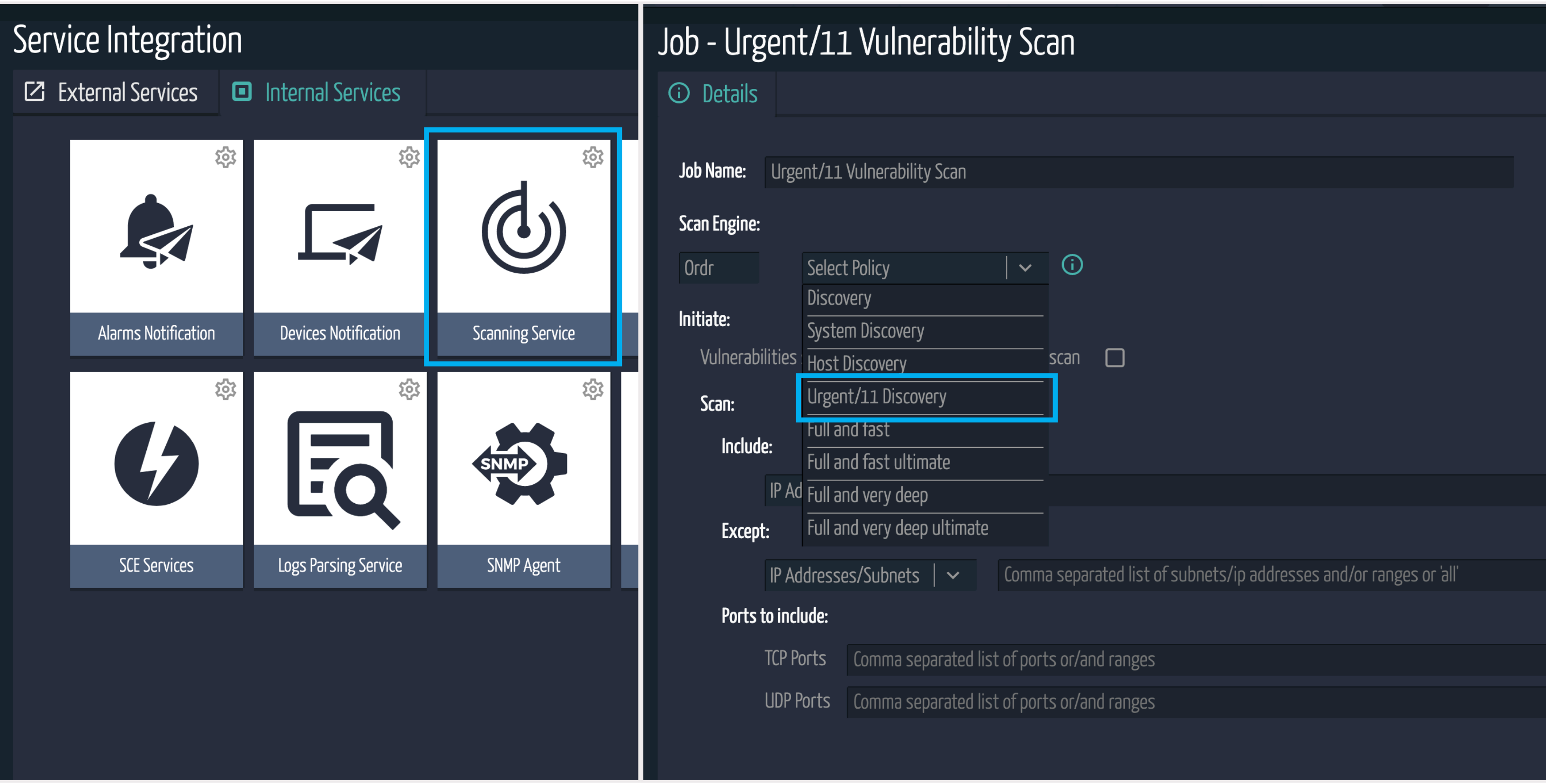
ORDR SECURITY BULLETIN

Identifying Devices Vulnerable to URGENT/11

Ordr exercises a combination of manufacturer advisories and proactive probing to track devices that are vulnerable to URGENT/11. This information is compared to any matching inventory in Ordr SCE customer environments automatically through a new URGENT/11 feed service. This ensures organizations will be continually apprised for vulnerabilities as soon as the information is available. A major challenge to reliance on manufacturer disclosure is the presence of countless variants of the IPnet implementation from numerous manufacturers that have licensed the IPnet TCP/IP stack over the years. What's even more challenging is the length and breadth of the impact affecting not just bio-med devices but also facility, security, industrial control devices, and more. This makes full and reliable disclosure elusive, distant or in some cases non-existent.

To help guarantee organizations can accurately identify any system vulnerable to URGENT/11, whether it has been published or not, Ordr has built an URGENT/11 active scanner. The scanner dynamically identifies, or verifies, at risk devices. The scanner is "light and tight" minimal operational impact, and it can be tuned to only scan specific device types or areas of the network.

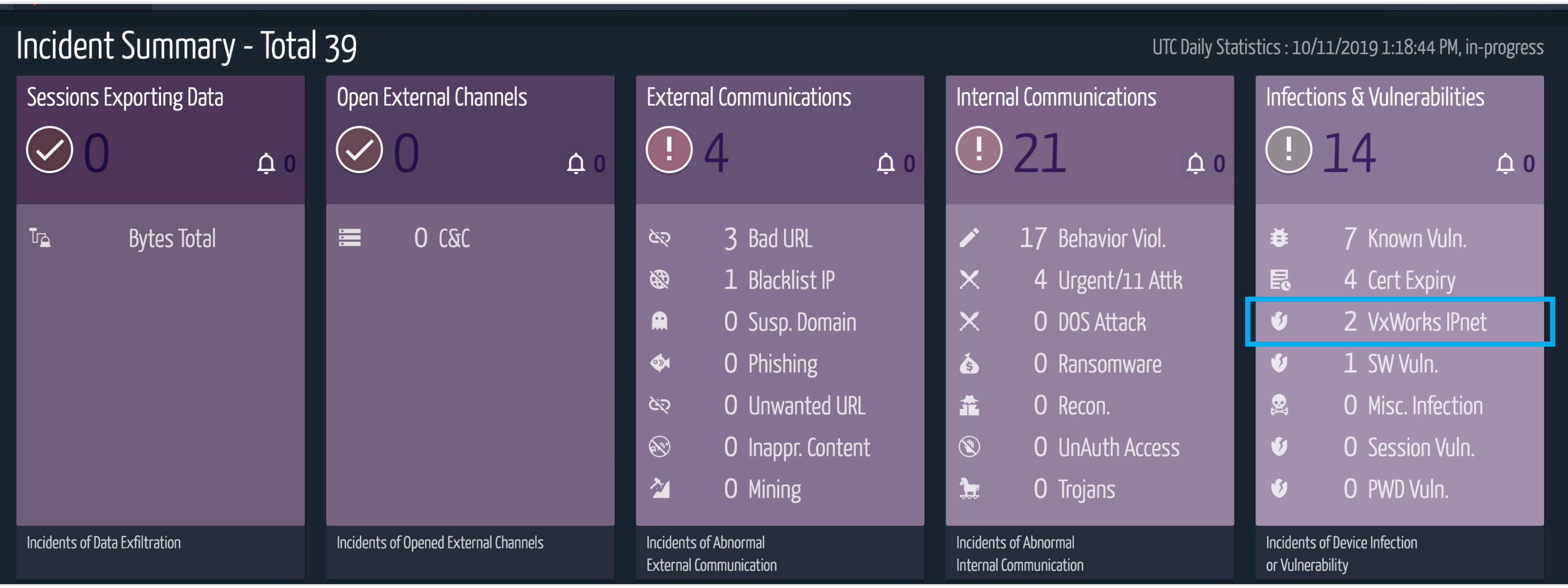
Below is an example of how customer can initiate vulnerability scan, looking for URGENT/11 impacted endpoints.



Job Name: Urgent/11 Vulnerability Scan

Scan Engine: Ordr

When devices are discovered that are vulnerable to URGENT/11, either due to the feed service or the active scanner, they are called-out on the Ordr Security Dashboard.



Incident Summary - Total 39

UTC Daily Statistics : 10/11/2019 1:18:44 PM, in-progress

Sessions Exporting Data
✓ 0 🔔 0
Bytes Total
Incidents of Data Exfiltration

Open External Channels
✓ 0 🔔 0
0 C&C
Incidents of Opened External Channels

External Communications
! 4 🔔 0

Count	Incident
3	Bad URL
1	Blacklist IP
0	Susp. Domain
0	Phishing
0	Unwanted URL
0	Inappr. Content
0	Mining

Incidents of Abnormal External Communication

Internal Communications
! 21 🔔 0

Count	Incident
17	Behavior Viol.
4	Urgent/11 Attk
0	DOS Attack
0	Ransomware
0	Recon.
0	UnAuth Access
0	Trojans

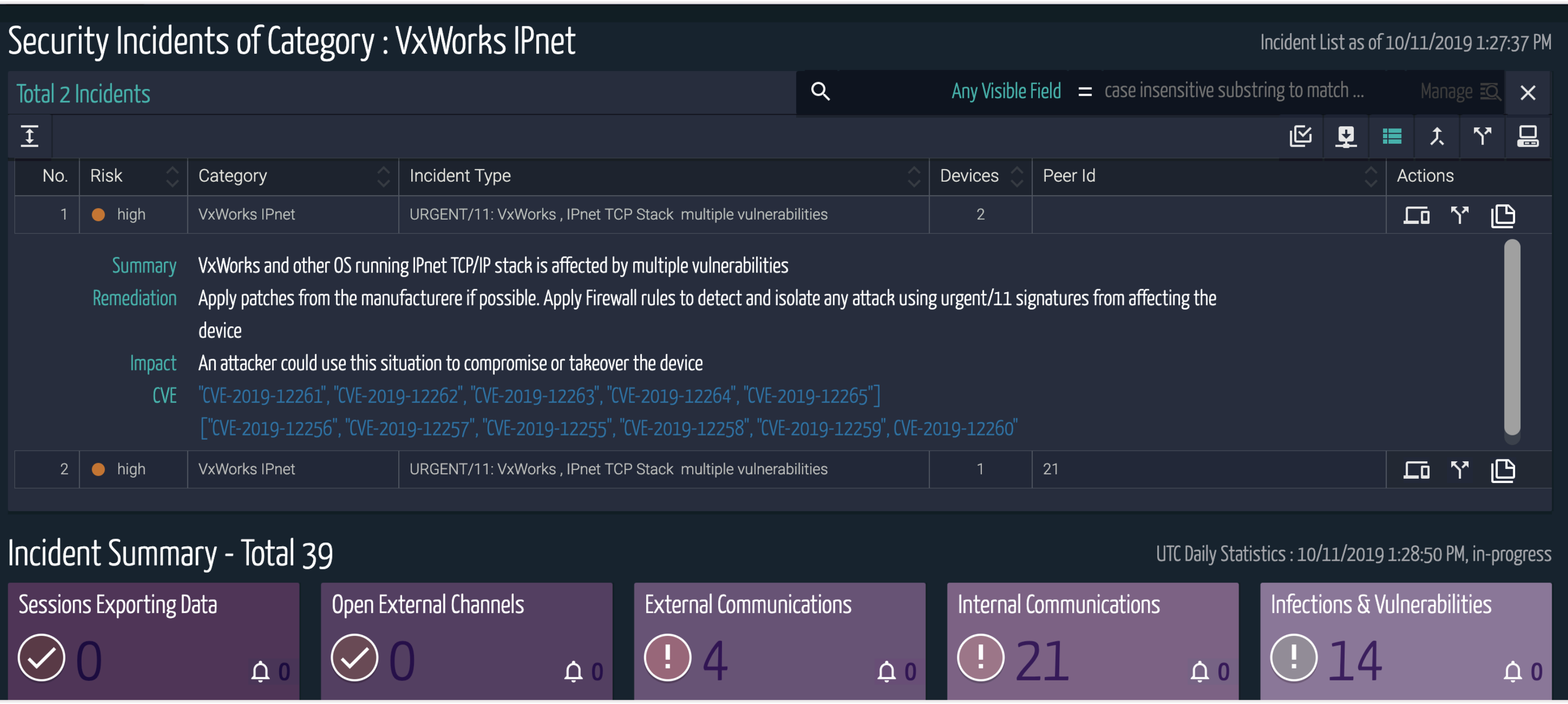
Incidents of Abnormal Internal Communication

Infections & Vulnerabilities
! 14 🔔 0

Count	Incident
7	Known Vuln.
4	Cert Expiry
2	VxWorks IPnet
1	SW Vuln.
0	Misc. Infection
0	Session Vuln.
0	PWD Vuln.

Incidents of Device Infection or Vulnerability

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



Security Incidents of Category : VxWorks IPnet

Incident List as of 10/11/2019 1:27:37 PM

Total 2 Incidents

No.	Risk	Category	Incident Type	Devices	Peer Id	Actions
1	● high	VxWorks IPnet	URGENT/11: VxWorks , IPnet TCP Stack multiple vulnerabilities	2		
2	● high	VxWorks IPnet	URGENT/11: VxWorks , IPnet TCP Stack multiple vulnerabilities	1	21	

Summary VxWorks and other OS running IPnet TCP/IP stack is affected by multiple vulnerabilities

Remediation Apply patches from the manufacturere if possible. Apply Firewall rules to detect and isolate any attack using urgent/11 signatures from affecting the device

Impact An attacker could use this situation to compromise or takeover the device

CVE "CVE-2019-12261", "CVE-2019-12262", "CVE-2019-12263", "CVE-2019-12264", "CVE-2019-12265"]
["CVE-2019-12256", "CVE-2019-12257", "CVE-2019-12255", "CVE-2019-12258", "CVE-2019-12259", CVE-2019-12260"

Incident Summary - Total 39

UTC Daily Statistics : 10/11/2019 1:28:50 PM, in-progress

Sessions Exporting Data ✓ 0 🔔 0

Open External Channels ✓ 0 🔔 0

External Communications ! 4 🔔 0

Internal Communications ! 21 🔔 0

Infections & Vulnerabilities ! 14 🔔 0

Reports can be generated for auditing or reporting purposes from Ordr SCE.

Please note that Ordr SCE integrates with external vulnerability assessment tools such as Tenable and Rapid7. Organizations using those tools to detect devices vulnerable to URGENT/11 can integrate them into the Ordr SCE inventory and security dashboard.

Detect Active Exploitation of URGENT/11

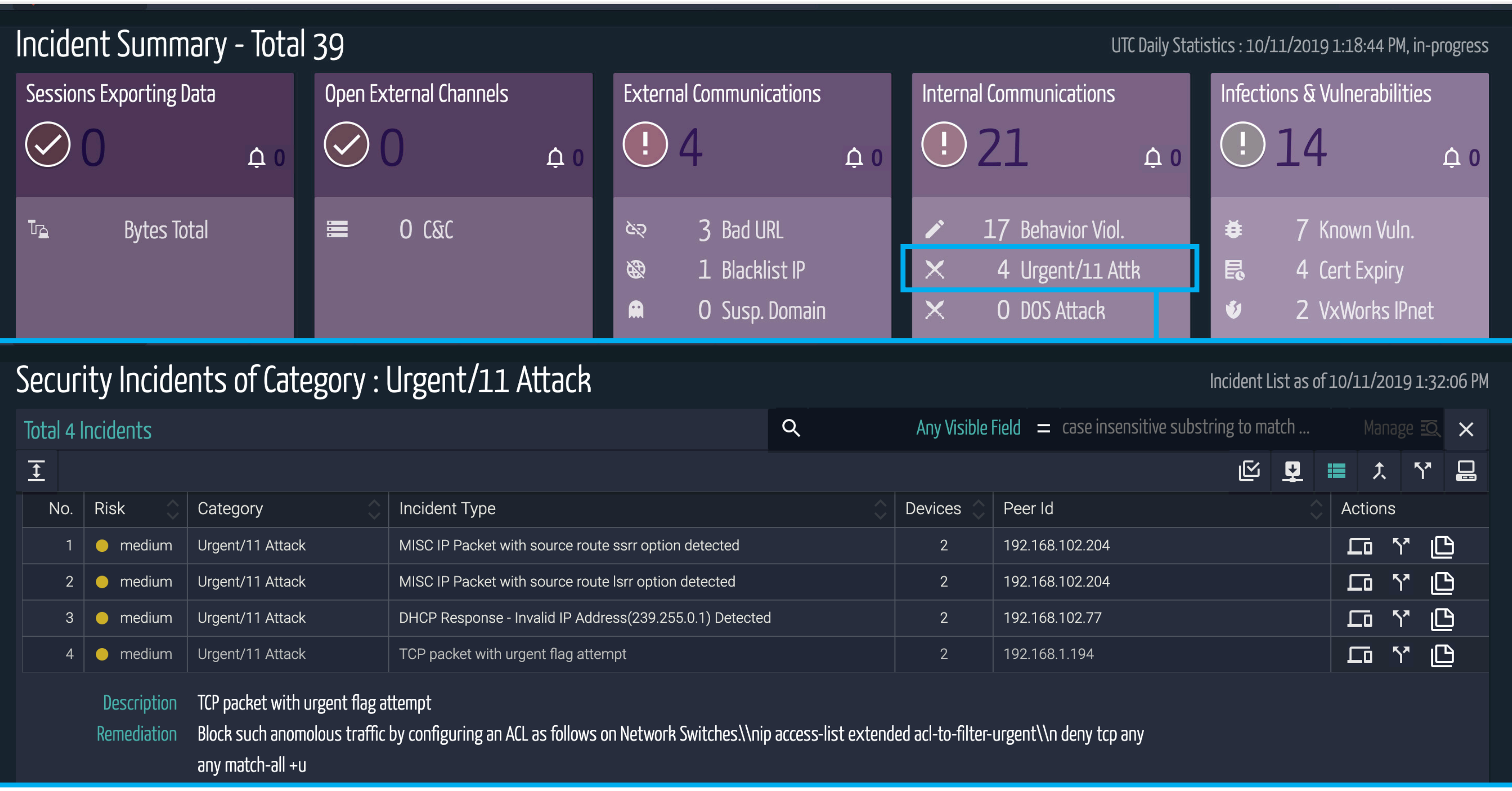
Ordr SCE has a built-in Network Intrusion Detection System (NIDS) engine which monitors traffic traveling throughout the network. The NIDS rules are updated to detect the URGENT/11 vulnerability behavior. This is a distinct advantage over reliance on traditional firewalls that typically monitor traffic coming through north-south choke point such as the Internet Edge. In order to exploit most of the URGENT/11 vulnerabilities, attackers need to be on the same segment or in the same VLAN rendering traditional firewall-based solutions ineffective. Ordr SCE monitors every device communication passively and checks against its 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 URGENT/11 attacks, as shown in the following table, and they are all included in the Ordr NIDS engine.

CVES	CVSS	DETAILS
CVE-2019-12256	9.8	Stack overflow in parsing of IPv4 packets' IP options
CVE-2019-12255	9.8	TCP Urgent Pointer = 0 leads to integer underflow VxWorks versions 6.5 to 6.9.3
CVE-2019-12260	9.8	TCP Urgent Pointer state confusion caused by malformed TCP AO option VxWorks versions 6.9.4 and above
CVE-2019-12261	8.8	TCP Urgent Pointer state confusion during connect() to a remote VxWorks versions 6.6 and above
CVE-2019-12263	8.1	TCP Urgent Pointer state confusion due to a race condition VxWorks versions 6.7 and above
CVE-2019-12257	8.8	Heap overflow in DHCP Offer/Ack parsing inside ipdhcpc

CVES	CVSS	DETAILS
CVE-2019-12258	7.5	DoS (Denial of Service) of TCP connection via malformed TCP options
CVE-2019-12262	7.1	Handling of unsolicited Reverse ARP replies (logic flaw)
CVE-2019-12264	7.1	Logic flaw in IPv4 assignment by ipdhcpc DHCP client
CVE-2019-12259	6.3	DoS via NULL dereference in IGMP parsing
CVE-2019-12265	5.3	IGMP Information leak via IGMPv3 specific membership report

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.



Incident Summary - Total 39

UTC Daily Statistics : 10/11/2019 1:18:44 PM, in-progress

Sessions Exporting Data	Open External Channels	External Communications	Internal Communications	Infections & Vulnerabilities
✓ 0 🔔 0	✓ 0 🔔 0	! 4 🔔 0	! 21 🔔 0	! 14 🔔 0
Bytes Total	0 C&C	3 Bad URL 1 Blacklist IP 0 Susp. Domain	17 Behavior Viol. 4 Urgent/11 Attk 0 DOS Attack	7 Known Vuln. 4 Cert Expiry 2 VxWorks IPnet

Security Incidents of Category : Urgent/11 Attack

Incident List as of 10/11/2019 1:32:06 PM

Total 4 Incidents

No.	Risk	Category	Incident Type	Devices	Peer Id	Actions
1	● medium	Urgent/11 Attack	MISC IP Packet with source route ssrr option detected	2	192.168.102.204	
2	● medium	Urgent/11 Attack	MISC IP Packet with source route lsrr option detected	2	192.168.102.204	
3	● medium	Urgent/11 Attack	DHCP Response - Invalid IP Address(239.255.0.1) Detected	2	192.168.102.77	
4	● medium	Urgent/11 Attack	TCP packet with urgent flag attempt	2	192.168.1.194	

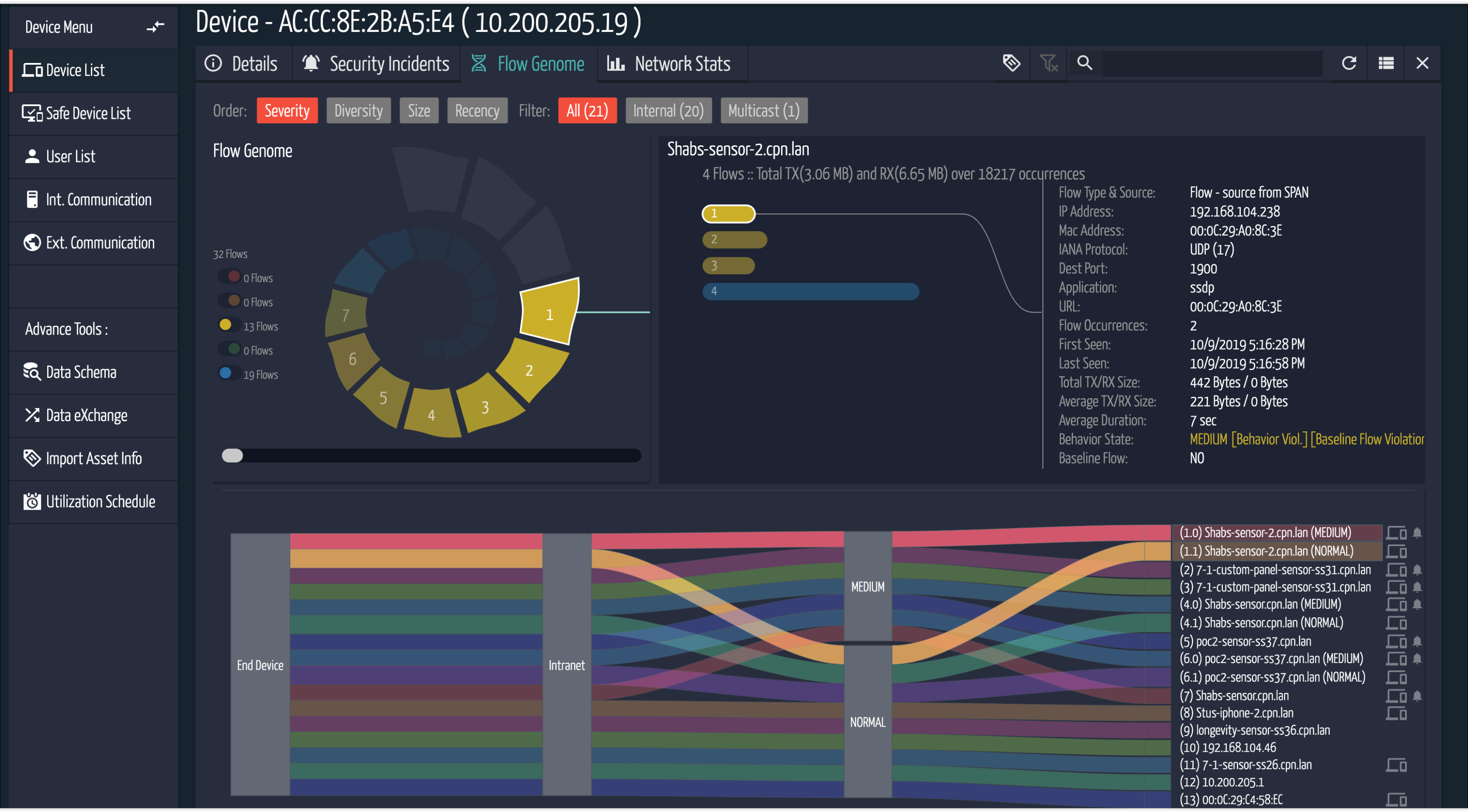
Description TCP packet with urgent flag attempt

Remediation Block such anomolous traffic by configuring an ACL as follows on Network Switches.\\nip access-list extended acl-to-filter-urgent\\n deny tcp any any match-all +u

Optionally, security incidents can be shared with Security Information and Event Management (SIEM) tools like Splunk, 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 to URGENT/11. If you have devices that cannot be patched in a timely fashion, Ordr SCE can implement microsegment as a compensating control to limit the surface area of attack while ensuring the device's continued operation.



Device - AC:CC:8E:2B:A5:E4 (10.200.205.19)

Shabs-sensor-2.cpn.lan

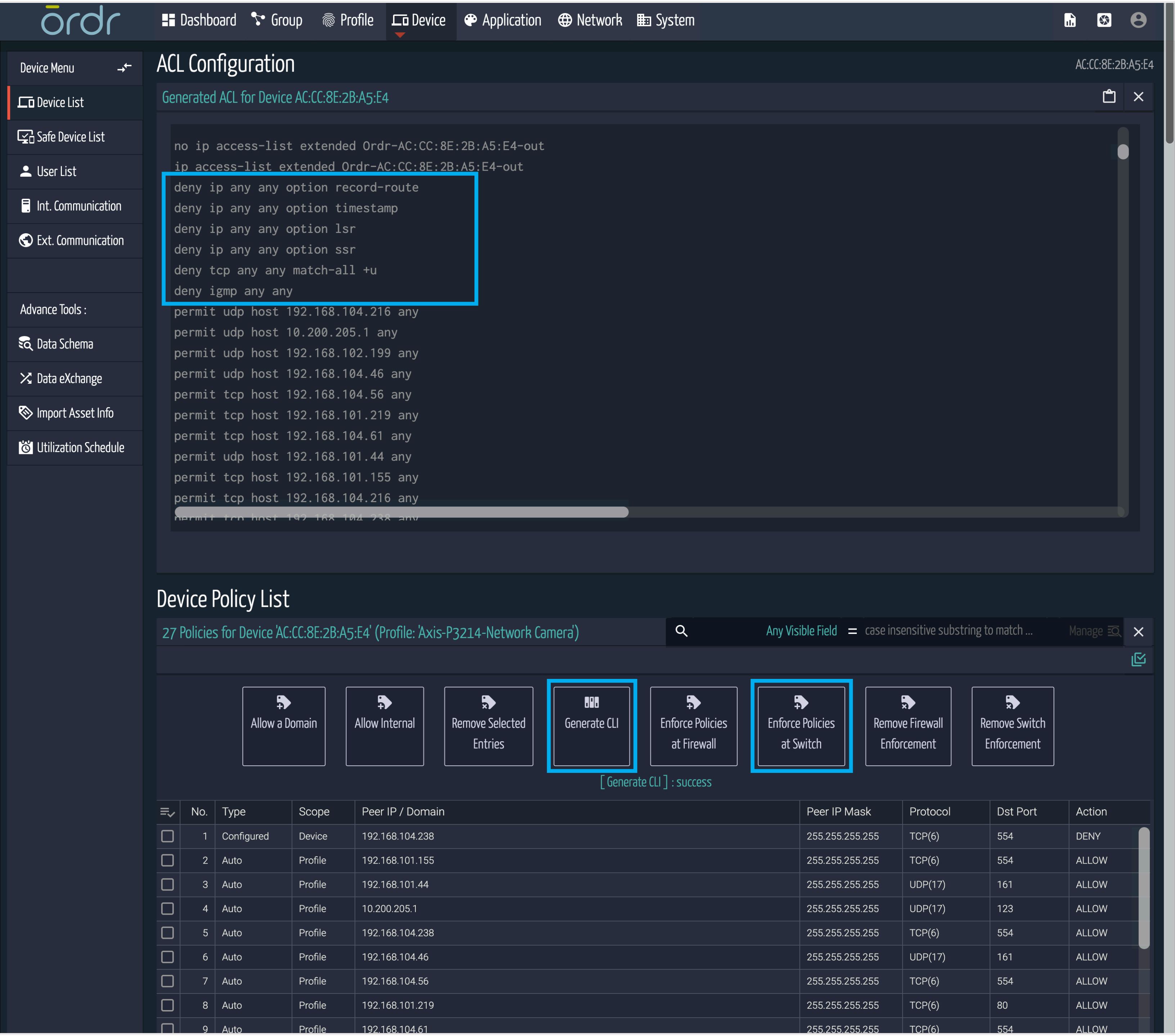
4 Flows :: Total TX(3.06 MB) and RX(6.65 MB) over 18217 occurrences

Flow Type & Source: Flow - source from SPAN
IP Address: 192.168.104.238
Mac Address: 00:0C:29:A0:8C:3E
IANA Protocol: UDP (17)
Dest Port: 1900
Application: ssdp
URL: 00:0C:29:A0:8C:3E
Flow Occurrences: 2
First Seen: 10/9/2019 5:16:28 PM
Last Seen: 10/9/2019 5:16:58 PM
Total TX/RX Size: 442 Bytes / 0 Bytes
Average TX/RX Size: 221 Bytes / 0 Bytes
Average Duration: 7 sec
Behavior State: MEDIUM [Behavior Viol.] [Baseline Flow Violatior
Baseline Flow: NO

(1.0) Shabs-sensor-2.cpn.lan (MEDIUM)
(1.1) Shabs-sensor-2.cpn.lan (NORMAL)
(2) 7-1-custom-panel-sensor-ss31.cpn.lan
(3) 7-1-custom-panel-sensor-ss31.cpn.lan
(4.0) Shabs-sensor.cpn.lan (MEDIUM)
(4.1) Shabs-sensor.cpn.lan (NORMAL)
(5) poc2-sensor-ss37.cpn.lan
(6.0) poc2-sensor-ss37.cpn.lan (MEDIUM)
(6.1) poc2-sensor-ss37.cpn.lan (NORMAL)
(7) Shabs-sensor.cpn.lan
(8) Stus-iphone-2.cpn.lan
(9) longevity-sensor-ss36.cpn.lan
(10) 192.168.104.46
(11) 7-1-sensor-ss26.cpn.lan
(12) 10.200.205.1
(13) 00:0C:29:C4:58:EC

The safeguard can be achieved by provisioning whitelist security policies with Access Control List (ACL) based on device behaviors observed by Ordr SCE. The policy enforcement can enabled directly from Ordr SCE and enforced directly in the network on switches and wireless controllers, sent to NAC solutions such as Cisco Identity Services Engine (ISE) or HPE Aruba ClearPass, or protected with zone-based security at firewalls including Palo Alto Networks, Check Point, Fortinet, and Cisco.

In case of URGENT/11, for instance, Ordr SCE automatically generates appropriate ACL denying specific TCP flags used in URGENT/11 vulnerabilities. This process is typically the most time-consuming part of the protection as it takes multiple efforts to combine device visibility and device behavior to build right security policies.



ACL Configuration

AC:CC:8E:2B:A5:E4

Generated ACL for Device AC:CC:8E:2B:A5:E4

```
no ip access-list extended Ordr-AC:CC:8E:2B:A5:E4-out
ip access-list extended Ordr-AC:CC:8E:2B:A5:E4-out
deny ip any any option record-route
deny ip any any option timestamp
deny ip any any option lsr
deny ip any any option ssr
deny tcp any any match-all +u
deny igmp any any
permit udp host 192.168.104.216 any
permit udp host 10.200.205.1 any
permit udp host 192.168.102.199 any
permit udp host 192.168.104.46 any
permit tcp host 192.168.104.56 any
permit tcp host 192.168.101.219 any
permit tcp host 192.168.104.61 any
permit udp host 192.168.101.44 any
permit tcp host 192.168.101.155 any
permit tcp host 192.168.104.216 any
permit tcp host 192.168.104.238 any
```

Device Policy List

27 Policies for Device 'AC:CC:8E:2B:A5:E4' (Profile: 'Axis-P3214-Network Camera')

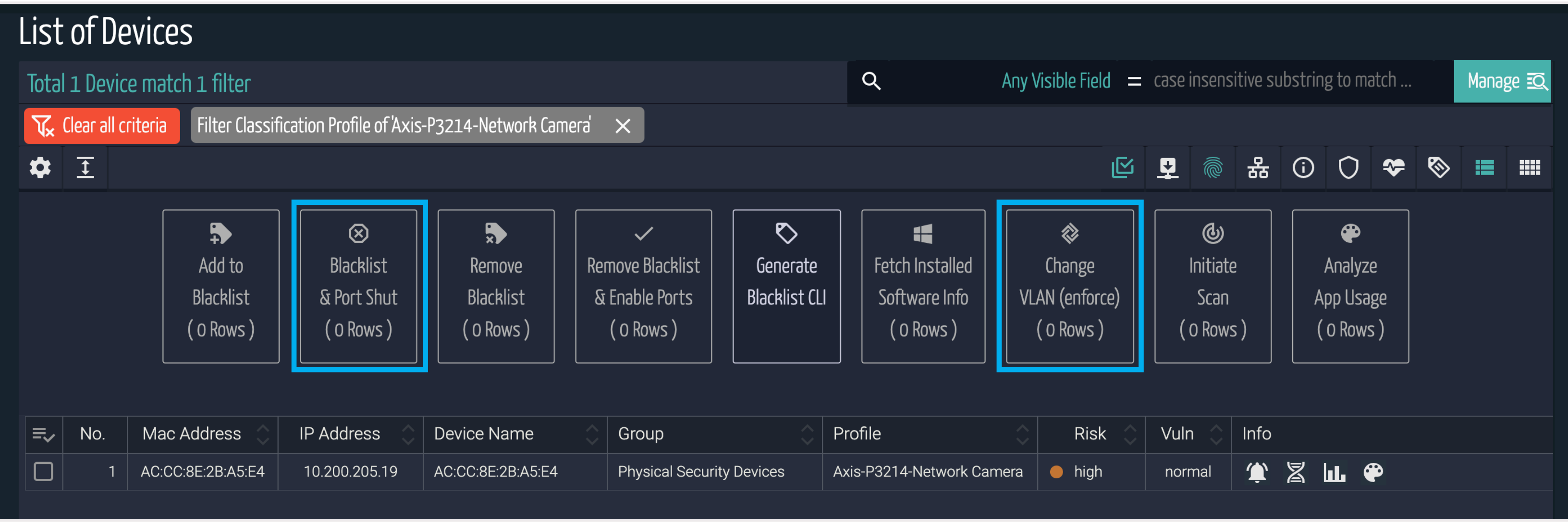
Any Visible Field
=
case insensitive substring to match ...
Manage
Allow a Domain
Allow Internal
Remove Selected Entries
Generate CLI
Enforce Policies at Firewall
Enforce Policies at Switch
Remove Firewall Enforcement
Remove Switch Enforcement

[Generate CLI] : success

	No.	Type	Scope	Peer IP / Domain	Peer IP Mask	Protocol	Dst Port	Action
☐	1	Configured	Device	192.168.104.238	255.255.255.255	TCP(6)	554	DENY
☐	2	Auto	Profile	192.168.101.155	255.255.255.255	TCP(6)	554	ALLOW
☐	3	Auto	Profile	192.168.101.44	255.255.255.255	UDP(17)	161	ALLOW
☐	4	Auto	Profile	10.200.205.1	255.255.255.255	UDP(17)	123	ALLOW
☐	5	Auto	Profile	192.168.104.238	255.255.255.255	TCP(6)	554	ALLOW
☐	6	Auto	Profile	192.168.104.46	255.255.255.255	UDP(17)	161	ALLOW
☐	7	Auto	Profile	192.168.104.56	255.255.255.255	TCP(6)	554	ALLOW
☐	8	Auto	Profile	192.168.101.219	255.255.255.255	TCP(6)	80	ALLOW
☐	9	Auto	Profile	192.168.104.61	255.255.255.255	TCP(6)	554	ALLOW

Take Swift Action

In cases where Ordr SCE sees suspicion activities from compromised endpoints, operator can immediately initiate the remediation process by sending appropriate policy change to the network or firewall to isolate and quarantine offending devices. Sample remediations may include the use of quarantine Virtual LANs (VLANs) or denying network access to the endpoint completely through blacklisting and/or shutting down the endpoint's network port. This can be performed directly from Ordr SCE or automated through NAC tools like Cisco ISE and HPE Aruba ClearPass.


List of Devices
Total 1 Device match 1 filter
Any Visible Field = case insensitive substring to match ...
Manage
Clear all criteria
Filter Classification Profile of 'Axis-P3214-Network Camera'
Add to Blacklist (0 Rows)
Blacklist & Port Shut (0 Rows)
Remove Blacklist (0 Rows)
Remove Blacklist & Enable Ports (0 Rows)
Generate Blacklist CLI
Fetch Installed Software Info (0 Rows)
Change VLAN (enforce) (0 Rows)
Initiate Scan (0 Rows)
Analyze App Usage (0 Rows)

	No.	Mac Address	IP Address	Device Name	Group	Profile	Risk	Vuln	Info
☐	1	AC:CC:8E:2B:A5:E4	10.200.205.19	AC:CC:8E:2B:A5:E4	Physical Security Devices	Axis-P3214-Network Camera	● high	normal	

Conclusion

URGENT/11 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 URGENT/11 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.

ōrdr

take control.

info@ordr.net
www.ordr.net ✉

2445 Augustine Drive Suite 601
Santa Clara, CA 95054