2022-2023 Educational Webinar Series

Cybersecurity and Asset Discovery Tools – Lessons Learnt

October 13, 2022

Speakers:

Chad Waters
Senior Cybersecurity Engineer
cwaters@ecri.org

Kristopher Kusche
Senior VP and System Chief Information Officer
KuscheK@amc.edu

ACCE gratefully acknowledges the sponsorship of the 2022-2023 Educational Webinar series by

About the moderator

Caroline Chyc-Olesiak, BS

Caroline Chyc-Olesiak is Clinical Engineer at Information Technology Services, Yale New Haven Health.

Caroline is currently working in the Yale New Haven Health System as a Clinical Engineer. My duties are ultimately to improve the quality of service for patients by helping healthcare workers utilize devices correctly. In these unprecedented times, cost is a critical component of any decisions for our department and the whole healthcare system.

Logistics

❖All attendees have their microphones muted during the presentation.

❖Questions to the panelists must be submitted via the "Q&A" feature in Zoom at any time. They will be addressed at the Q&A portion.

❖If there is any urgent issue, please use the "chat" feature to communicate with the host/moderator.

❖Please remember to complete the webinar evaluation after attending. A link will be provided at the end.

About the Speaker

Kris Kusche

Senior VP and System Chief Information Officer

ALBANY MEDICAL CENTER

Kristopher Kusche joined the Albany Medical Center in 1993 where he currently serves as the Senior VP and System Chief Information Officer responsible for all IT, Medical Device and PACS related operations across the 5-hospital campus Albany Med Health System. Mr. Kusche's previous role was as VP and Chief Information Security Officer responsible for security policy, operations, investigation, enforcement and compliance. Prior executive roles included management of all technology operations, clinical systems, data and system integration and data architecture teams. Mr. Kusche earned his bachelor of science and master of engineering degrees (M.Eng.), both in Biomedical Engineering, from the Rensselaer Polytechnic Institute in Troy, New York, and currently holds certifications as both a Certified Information Systems Security Professional (CISSP) and HealthCare Information Security and Privacy Practitioner (HCISPP) from the International Information Systems Security Certification Consortium (ISC2) and as a Certified Professional in Healthcare Information and Management Systems (CPHIMS) from the Healthcare Information and Management Systems Society (HIMSS).

About the Speaker

Chad Waters,

Senior Cybersecurity engineer

ECRI

Chad Waters is currently the Senior Cybersecurity Engineer, Device Evaluation group at ECRI. Chad is responsible for:

- Security assessment of devices
- Security alerts
- Guidance articles

10+ years experience as Network Security Engineer in a hospital system.

BS in Information Technology from Rochester Institute of Technology.

Conflict of Interest Statement

Kristopher Kusche, M.Eng., CISSP, CPHIMS, FHIMSS, HCISPP

The presenter has no real or apparent conflicts of interest to report and affirms that no remuneration or other compensation is being received for this presentation. In no way does the mention of specific vendors or products imply any endorsement of that vendor or product.

Conflict of Interest Statement

Chad Waters

The presenter has no real or apparent conflicts of interest to report and affirms that no remuneration or other compensation is being received for this presentation. In no way does the mention of specific vendors or products imply any endorsement of that vendor or product.

Session Description

Asset discovery tools or Internet of Medical Things (IoMT) security solutions have become an essential tool for many healthcare organizations in managing their network connected assets. These software and hardware systems aim to help healthcare facilities improve their security posture and ensure visibility into the organizations assets through monitoring network traffic. Many facilities have implemented one these solutions and are well on their way in optimizing their use.

Join this ACCE Educational Webinar to learn more about the IoMT solutions and to hear lessons learnt from a healthcare facility's journey on implementing and utilizing these systems.

Agenda

- Discuss the cybersecurity landscape for the Healthcare sector
- Discuss medical devices and their characteristics to understand how they differ from traditional information technology
- Review gaps in current programmatic approaches to managing the cybersecurity of medical devices
- Review a current IoT management toolset used to monitor medical device cybersecurity via s sample case study
- Open discussion and questions

ECRI Top 10 Health Technology Hazards

- **2022** - #1. Cybersecurity Attacks Can Disrupt Healthcare Delivery, Impacting Patient Safety
- **2021** - #7. Vulnerabilities in third-party software components present cybersecurity challenges
- **2020** - #7. Cybersecurity Risks in the Connected Home Healthcare Environment
- **2019** - #1. Hackers Can Exploit Remote Access to Systems, Disrupting Healthcare delivery
- **2018** - #1. Ransomware and Other Cybersecurity Threats
- **2017** - #6. Software Management Gaps Put Patients, and Patient Data, at Risk
- **2016** - #10. Misuse of USB Ports Can Cause Medical Devices to Malfunction
- **2015** - #9. Cybersecurity: Insufficient Protections for Medical Devices and Systems

Medical Device Security Challenges

- Whose responsibility is this?- IT, Security, HTM, CE
  - Fractured inventory and documentation
- Vulnerability scanning of production medical devices is not recommended
  - likelihood is low, but impact could be very high
- Typically cannot install AV/endpoint security on a device
- Vulnerability scoring, prioritization, patching cadences
  - Coordinated downtimes, a lot of compensating controls

IoMT Security Solutions offerings

- “passive scanning” – analyzing network traffic, not directly interacting medical devices
- Great at inventory *
- Vulnerability identification
- Behavioral anomaly detection
  - This device is doing something that it normally doesn’t do.
- Remediation (recommendation or automated)
- Utilization data

Organizational Considerations

- Determine who will be the users of this tool and get them involved in the evaluation
  - IT, Security, HTM, CE
  - Do you need utilization data?
  - Will this be used for OT devices as well (HVAC, facilities)
- Integrations with other tools in the environment
  - CMMS, SIEM, NAC, other security tools, network equipment
  - Do you want this tool make changes to the network?
- Network architecture factors
  - How many listening devices do you need to catch all the device traffic
  - Do you need third party network taps /packet brokers - $$$

Considerations

- How detailed is identification?
  - Device type -> Vendor/Model -> Serial # -> Firmware version
- Are vulnerability/ security incident detections accurate?
  - False positives may occur at first
- Vulnerability Prioritization and remediations?
  - Does it provide more than CVSS, what is the clinical risk?
  - Are the recommendations actionable?
  - Again, do you trust this tool to make changes to the network?

Why are we here?

With the rapid growth of medical devices in the interconnected healthcare landscape, Clinical Engineers and CISOs face the challenge of providing security for devices which look and act differently from traditional IT devices. The need to extend an IT security management program to medical devices is paramount to secure the HIT computing environment.

Why am I here?

Healthcare Information Technology executive with 25+ years of academic medical center experience

Master's degreed biomedical engineer with 25+ years of biomedical engineering management experience

15+ year academic medical center Chief Information Security Officer experience

CISSP, CPHIMS and HCISPP certified cybersecurity professional

Healthcare Cybersecurity Landscape

- Healthcare is the #1 breached sector
- In 2021 the healthcare industry had 330 breaches
    - Affecting ~28.1 M records
    - Represents 18% of total breaches across all sectors
    - 87% were attacks vs. errors; 31% of attacks were malware and only .2% were zero-day (i.e., we should be able to detect)
    - Average cost of a healthcare data breach - $9.23M
- Medical device counts may outpace traditional IT devices 2:1
- ~48% of medical devices are network connected

Sources:

1) *2021 End-of-Year Data Breach Report*, Identity Theft Resource Center, www.idtheftcenter.org
2) *2021 Cost of Data Breach Study*, Ponemon Institute, www.ponemon.org
3) *Medtech and the Internet of Medical Things*, Deloitte, https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Life-Sciences-Health-Care/gx-lshc-medtech-iomt-brochure.pdf

Medical Device Cybersecurity Landscape

The FDA says that with regards to mitigating cybersecurity risks

-“Medical device manufacturers (MDMs) are responsible for remaining vigilant about identifying risks and hazards associated with their medical devices, including risks related to cybersecurity.
- Health care delivery organizations (HDOs) should evaluate their network security and protect their hospital systems.
- Both MDMs and HDOs are responsible for putting appropriate mitigations in place to address patient safety risks and ensure proper device performance.”

Source:

1) *Cybersecurity,* Food and Drug Administration, https://www.fda.gov/medical-devices/digital-health/cybersecurity

What is a Medical Device

The FDA defines a medical device as an instrument or apparatus that is:

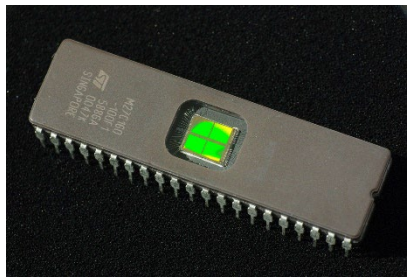
"intended for use in the diagnosis of disease or other conditions, or in the cure, mitigation, treatment, or prevention of disease…"

Source:

1) *Is The Product A Medical Device?,* Food and Drug Administration, https://www.fda.gov/medical-devices/classify-your-medical-device/product-medical-device

What makes a medical device different?

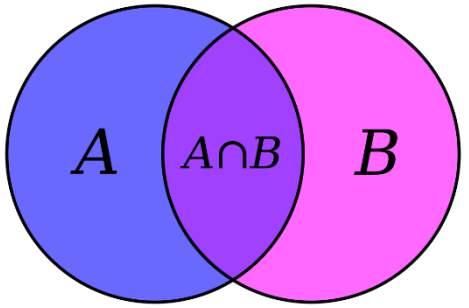
Technical Differences



- Embedded software on EEPROMs vs. volatile memory (i.e., can't be updated via normal patching mechanisms)
- Non-standard operating systems (e.g., vxWorks)
- Medical devices talk different languages (DICOM, HL7, Metagram) from IT devices
  - Normal toolsets can't adequately "see" medical devices or protocols which mean that medical devices are difficult to visualize, manage and secure

vs.

What makes a medical device different?



People and Process Differences

- CE and IT are not typically leadership-aligned
- CE and IT personnel have different skillsets
- Inventory intentions and uses are inherently different
  - CE inventories are “cradle to grave” focused on device risk and safety (i.e., regulatory safety inspection completion, recalls, failure incident and modal analysis)
  - IT inventories are asset tracking mechanisms used to better manage devices through characteristic detail (i.e., CPU, OS, software revision, patch levels)

What makes a medical device different?

Industry and Market Differences

- Medical devices are regulated by many agencies (e.g., FDA, CDRH, AABB, DoH, ACR, and others)
- Technology Refresh Cycle
  - Medical device replacement average 7-10 years
  - IT device replacement average 3-5 years
- Cost/Total Cost of Ownership
  - Desktop=$350, laptop=$1,500
  - IV pump=$6,000, Defibrillator=$15,000, Bedside Patient Monitor=$40,000, Anesthesia Machine=$75,000, Ultrasound=$250,000, MRI=$3M

Problem Restated

CEs and CISOs need to find a way to provide a cybersecurity program for networked devices that:

1) don’t behave like normal IT devices
2) can’t be monitored like normal IT devices
3) can’t be protected like normal IT devices
4) are supported by professionals with mismatched skillsets
5) have regulatory restrictions
6) have an extremely high TCO causing lags in technology currency

What We Need…People & Process

Technology leadership to reinvent medical device management

- Operational transformation of CE/IT relationship
- Application of IT security fundamentals to medical device management while maintaining CE rigor and safety focus
  - Security-focused product selection and contracting
  - Risk-assessed inventory inclusive of security related data (OS, firmware rev., model options)
- Cross-training of CE/IT staff for security harmonization

What We Need…Technology

New technology toolsets that “speak” medical device to prevent and detect breaches in the absence of the ability to apply typical IT preventive measures (i.e., anti-malware, encryption)

- Logical segmentation
- Real-time network visibility
- Device parameter discovery
- Vulnerability identification
- Behavior profiling and anomaly detection
- SIEM, Prevention and Alerting

Profiling

Defined as “the act or process of extrapolating information … based on known traits or tendencies”

To profile a networked medical device we look at its normal behaviors:

- network connection pairs
- communication protocols used
- resident applications
- traffic volumes and network payloads

Profiling can be used to identify anomalous behavior or increases in risk level which could indicate a compromise

Sources:

1) *Definition of Profiling,* Meriam-Webster Dictionary, https://www.merriam-webster.com/dictionary/profiling

Technology Scenario

Large Volume Infusion Pump

Scenario 1 - Normal Behavior

- Inventory discovery
- Network visibility
- Connectivity
- Protocol use
- Risk

Scenario 2 - Elevated Risk

Profile – IV Pump: Demographics

spectrum1016252@

Risk Level

Risk Score 26

Device Details

Network Details

Category	Infusion System
Profile	Sigma Spectrum Infusion System
Confidence Score	90
Last Activity	10:50 October 21, 2019

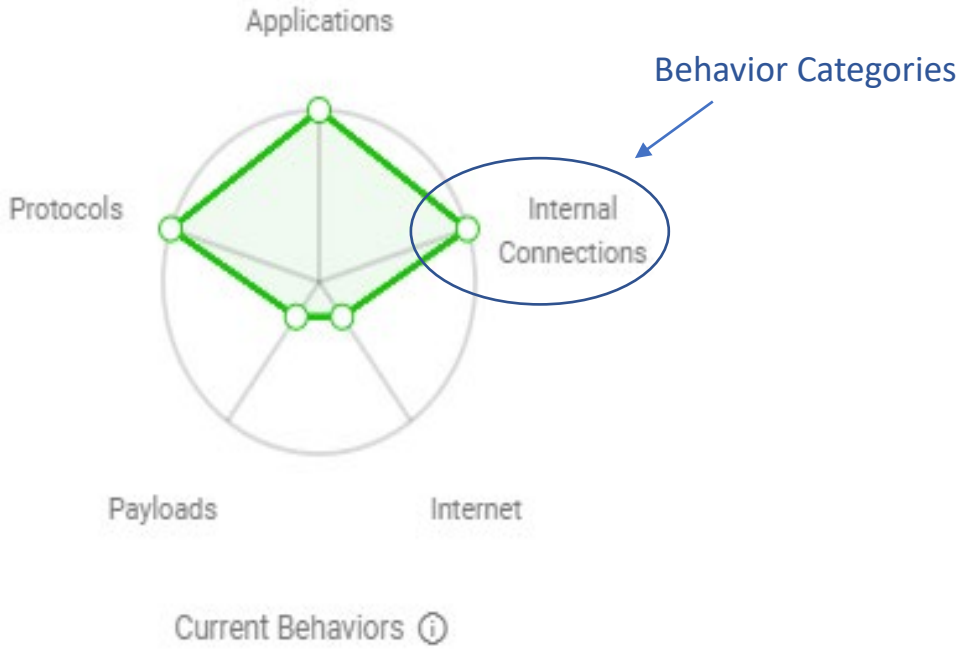
IDENTITY

Vendor	Baxter/SIGMA
Model	Sigma Spectrum
Serial Number	1016252
OS Group	Linux
OS Version	-/v6.02.07

MAC Address	00:40:9d:aa:c6:0d
IP Address	172.19.80.118
VLAN	712
Subnet	172.19.64.0/19
Wired - Wireless	wireless
DHCP	Yes
Connected Switch	WLC8540-C102-1 albanymedsecure-int
Access Point Name	AP3502-B2-12
Access Point IP	167.244.228.31

Site	Albany Med
International Access	No
Listening Ports	51243

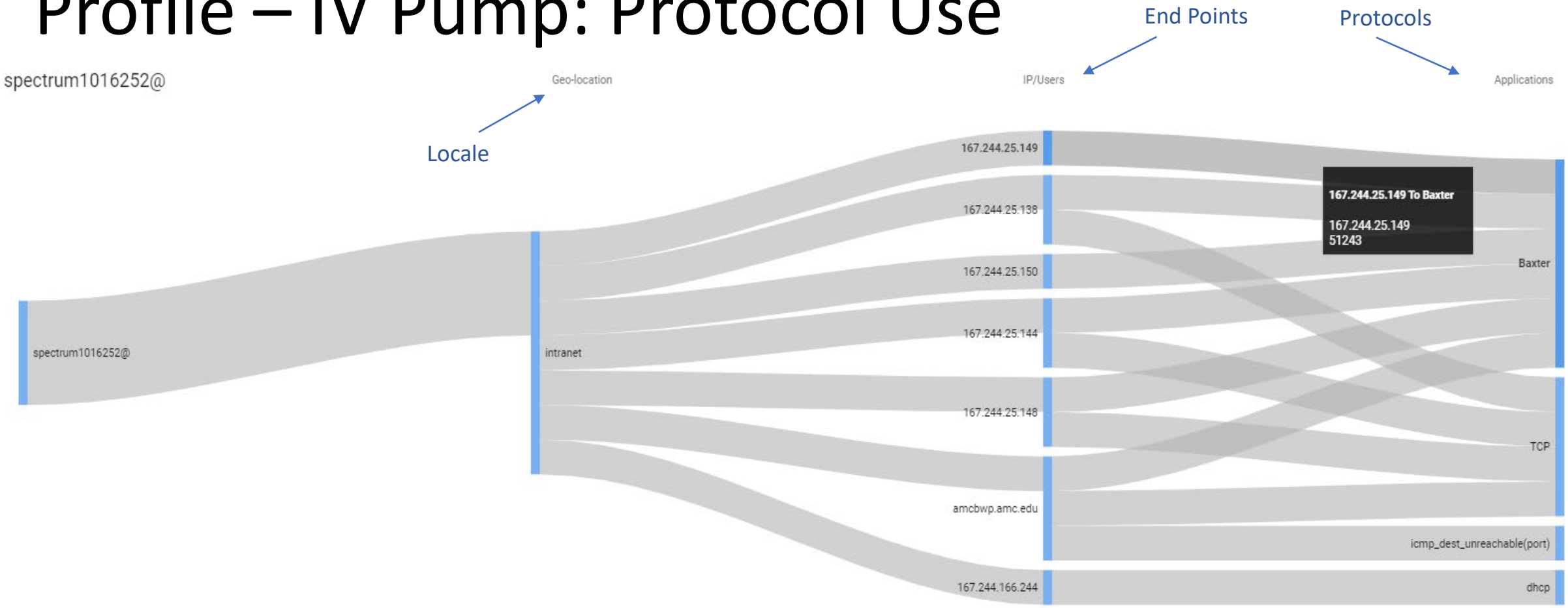
Profile – IV Pump: Behavior Profile (Normal)



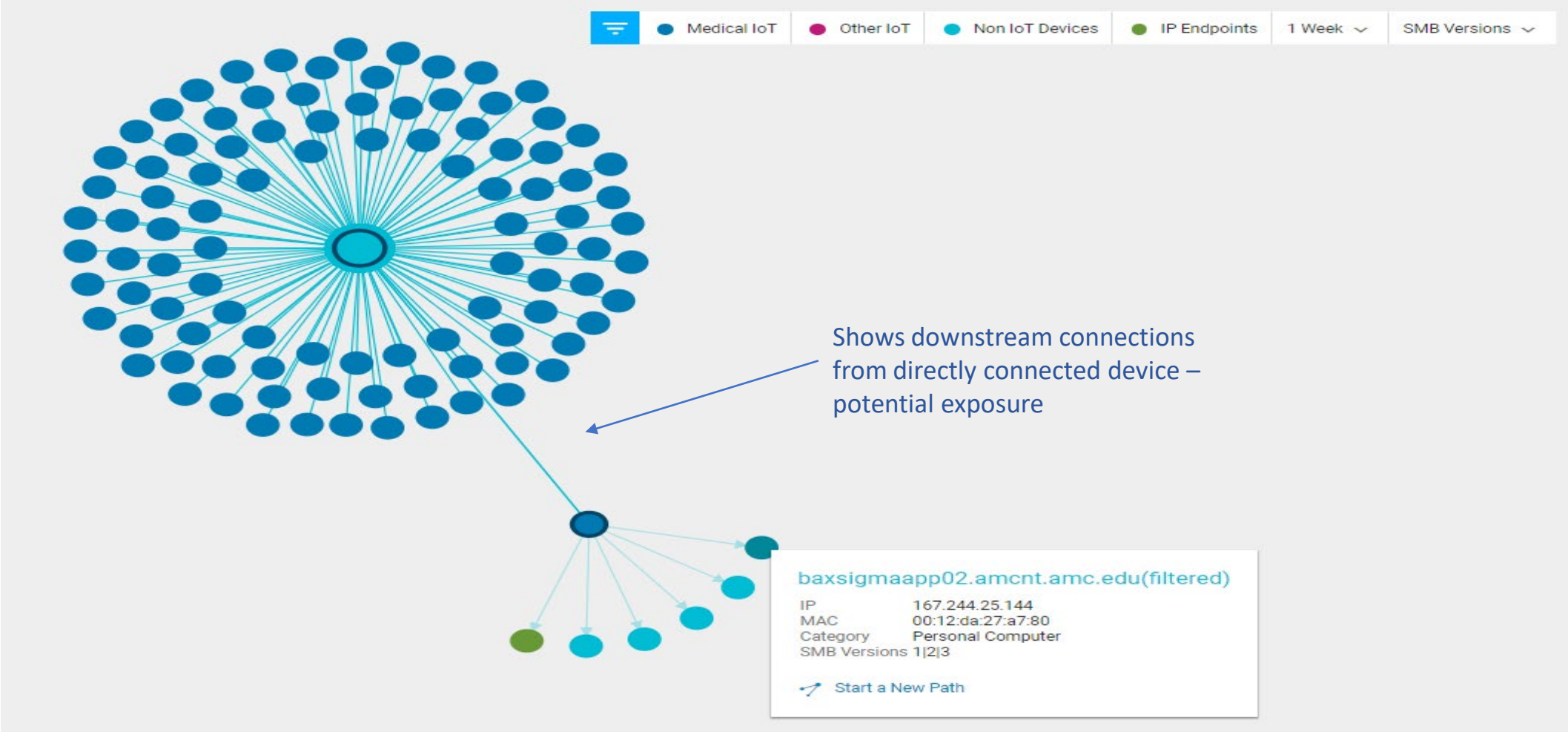
SECURITY

Risk Score	26
Baseline Modeling	
Anomaly Detection	Normal
First Seen	13:14 March 06, 2019
Last Activity	10:50 October 21, 2019

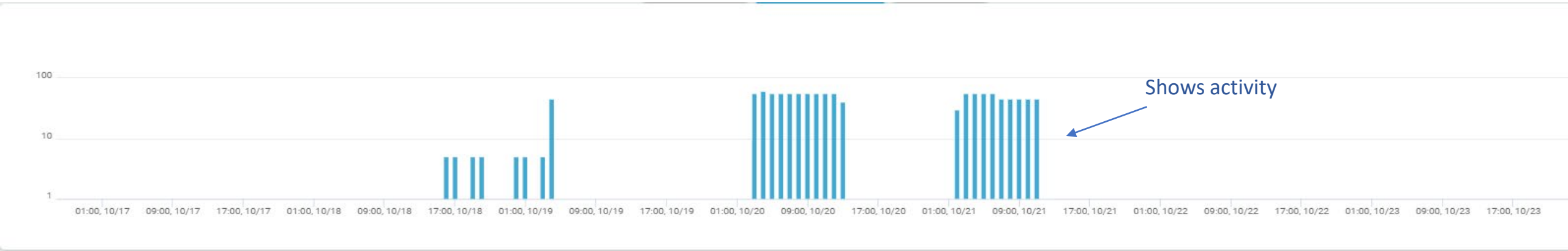
Profile – IV Pump: Protocol Use



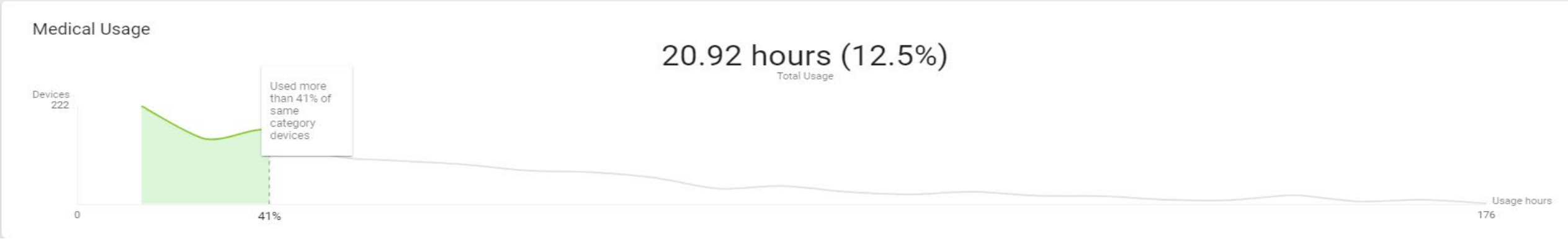
Profile – IV Pump: Network Neighborhood



Profile – IV Pump: Utilization (Connect Time)



Shows activity



Shows comparison of activity time vs. other IV Pumps

Profile – IV Pump: Elevated Risk (simulated)

spectrum797308@

Risk Score 76 Alert 1

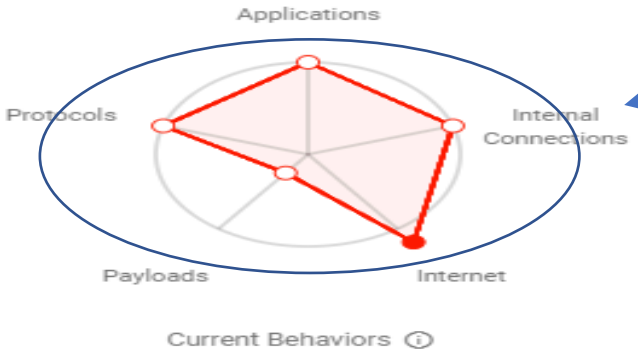
Increased Risk Score w/ Alert

Category	Infusion System
Profile	Sigma Spectrum Infusion System
Confidence Score	90
Last Activity	22:44 October 23, 2019

IDENTITY

Vendor	Baxter/SIGMA
Model	Sigma Spectrum
Serial Number	1015465
OS Group	Linux
OS Version	6.1/v6.02.07

Site	Albany Med
International Access	No
Listening Ports	51243, 21, 22

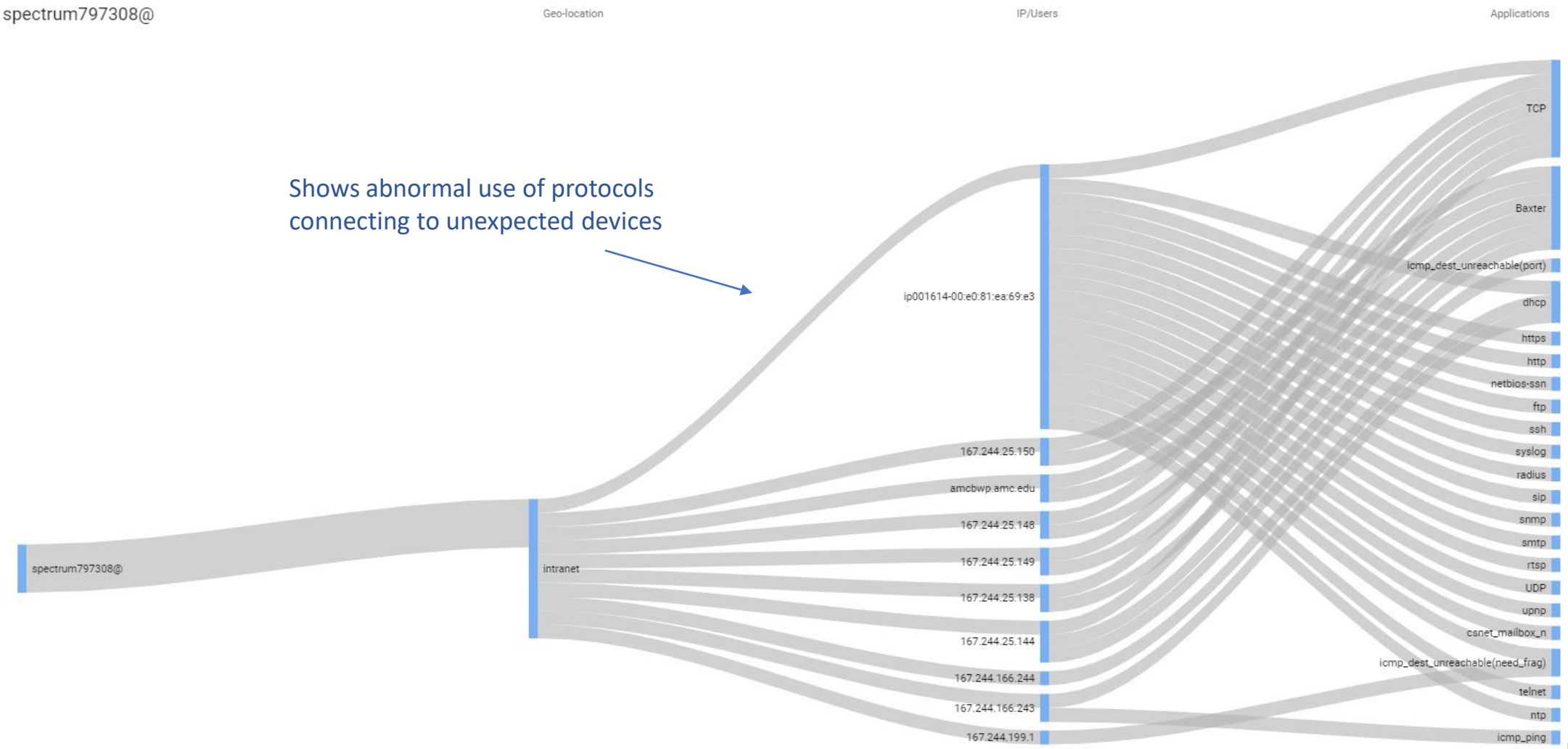


Anomalous behavior violations

SECURITY

Risk Score	76
Baseline Modeling	
Anomaly Detection	Normal
SMB Version	V2|3
First Seen	08:46 December 14, 2018
Last Activity	22:44 October 23, 2019

Profile – IV Pump: Elevated Risk (simulated)



Scenario Summary

Medical Device/IoT platform helps provide a means of managing medical device security by providing correlated metrics:

- Visibility of networked medical devices
- Physical location of device relative to network
- Real-time behavior profile and risk assessment
- Protocols being used by device
- Network traffic map by protocol
- Network neighborhood
- Device-specific activity and category utilization

What Else Do We Need?

Integration, Orchestration, Automation and Response

- Integration with network core for “echo-location”
- Connection to MEMS/CMMS for medical and IoT device inventory synchronization
- Integration to vulnerability scanning platform for on demand scans
- Feed data to SIEM for event correlation
- Integration to IDS/IPS for automated/ad hoc quarantine and response

Vulnerability/Risk Assessment (CVE, CVSS, MDS^2, etc.)

Vulnerability Discovery – “URGENT/11”

Severity	CVSS Score	Vulnerability Name	ICS-Cert	Source
	8.8	CVE-2019-12261		WindRiver
	9.8	CVE-2019-12260		WindRiver
	8.1	CVE-2019-12263		WindRiver
	8.8	CVE-2019-12257		WindRiver
	7.5	CVE-2019-12258		WindRiver
	5.4	CVE-2019-12265		WindRiver
	9.8	CVE-2019-12256		WindRiver
	9.8	CVE-2019-12255		WindRiver
	6.3	CVE-2019-12259		WindRiver
	7.1	CVE-2019-12262		WindRiver
	7.1	CVE-2019-12264		WindRiver

Vulnerability Impact – “URGENT/11” Impact

Vulnerabilities (11)

Active Filters: New Filter

Source

WindRiver ×

Severity	CVSS	Vulnerability	Source	Potentially Vuln. Devices	Description
Critical	9.8	CVE-2019-12255	WindRiver	622	TCP Urgent Pointer = 0 leads to integer underflow: A specially crafted TCP segment with the URG flag set can cause an overflow of the buffer passed to recv()...
Critical	9.8	CVE-2019-12256	WindRiver	622	Stack overflow in the parsing of IPv4 packets' IP options: A specially crafted IPv4 packet containing invalid encoded SSRR/LSRR (Strict Source and Record Ro...
Critical	9.8	CVE-2019-12260	WindRiver	622	TCP Urgent Pointer state confusion caused by malformed TCP AO (authentication option): A series of specially crafted TCP segments where the last one is a ...
High	8.8	CVE-2019-12257	WindRiver	622	Heap overflow in DHCP Offer/ACK parsing inside ipdhcpc: A specially crafted DHCP packet can cause an overflow of heap-allocated memory on VxWorks sys...
High	8.8	CVE-2019-12261	WindRiver	622	TCP Urgent Pointer state confusion during connect() to a remote host: A specially crafted connection response where both the FIN- and URG flags are set is s...
High	8.1	CVE-2019-12263	WindRiver	622	TCP Urgent Pointer state confusion due to race condition: This vulnerability relies on a race condition between the network task (tNet0) and the receiving appl...
High	7.5	CVE-2019-12258	WindRiver	622	DoS attack on TCP connections via malformed TCP options: A specially crafted packet containing illegal TCP options can result in the victim not just dropping...
High	7.1	CVE-2019-12262	WindRiver	622	Handling of unsolicited Reverse ARP replies (Logical Flaw): The RARP reception handler on the targeted device verifies that the packet is well formed but fails...
High	7.1	CVE-2019-12264	WindRiver	622	Logical flaw in IPv4 assignment by the DHCP client: The VxWorks DHCP client fails to properly validate that the offered IP address in a DHCP renewal or offer ...
Medium	6.3	CVE-2019-12259	WindRiver	622	DoS via NULL dereference in IGMP (Internet Group Management Protocol) parsing: This vulnerability requires that the API intended to assign a unicast addres...
Medium	5.4	CVE-2019-12265	WindRiver	622	IGMP Information leak via IGMPv3 specific membership report: An attacker can create a specially crafted and fragmented IGMPv3 query report, which can re...

Questions & Discussions

Enter your questions to the Q&A window

Thank You

Please complete the online evaluation form at
https://www.surveymonkey.com/r/session2_10-13-22

or scan the QR code