URGENT/11

Jack Marsal

Sr. Director, Product Marketing

ARMIS™

Forbes Billionaires Innovation Leadership Money Business Small Business Lifestyle BrandVoice Lists Advisor Featured

22,409 views | Jul 29, 2019, 11:00am

Critical 'Update Now' Warning Issued For VxWorks OS Inside 2 Billion IoT Devices

Zak Doffman Contributor
Cybersecurity
I write about security and surveillance.

ARMIS

URGENT/11

Impacted Wind River VxWorks

Real-Time Operating System (RTOS)

- 11 Critical Zero Day Vulnerabilities
  - 6 RCE/Takeover
  - 5 Denial of Service, Information Leaks, Logical Flaws
- All in the core networking stack (**IPnet**)
  - No User interaction required
  - Non-application specific

ARMIS

URGENT/11

Wind River VxWorks

Impacted

- All versions from VxWorks v6.5 forward
- Updates have been released

Not Impacted

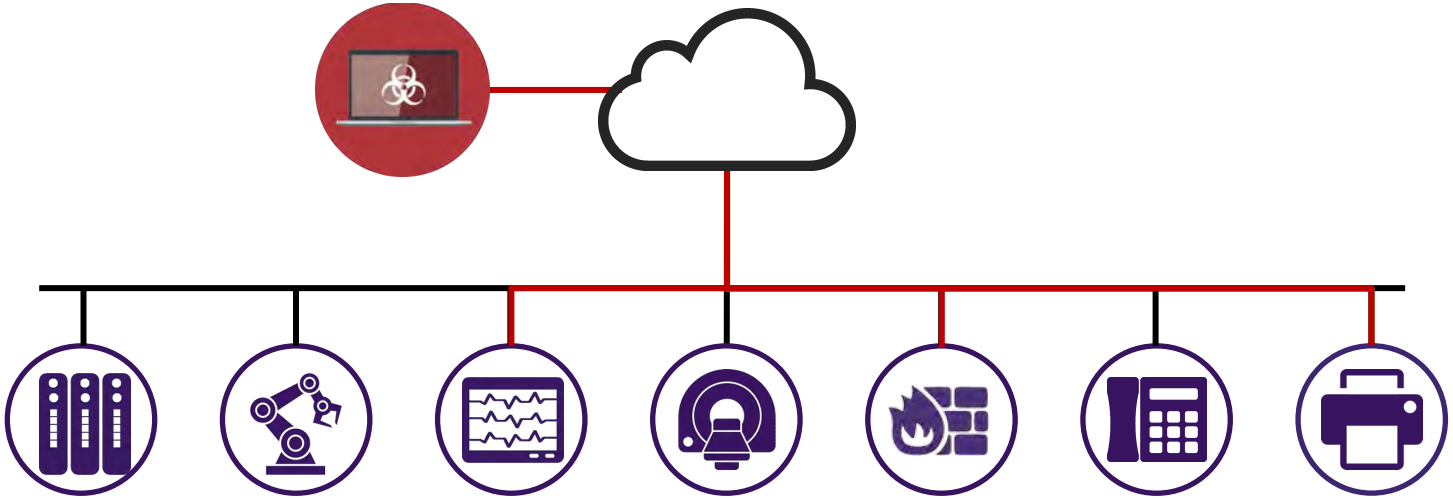
- VxWorks 653
- VxWorks Certified

URGENT/11 Devices Impacted

SCADA, industrial controllers, patient monitors, MRI machines, as well as firewalls, VOIP phones, printers, etc.

Siemens, ABB, Emerson Electric, Rockwell Automation, Mitsubishi Electronic, Samsung, Ricoh, Xerox, NEC, GE, and Arris, among others.

URGENT/11 Clarifying The Exposure



Even a device reaching outbound to the Internet could be taken over.

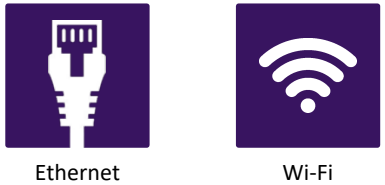
URGENT/11

Every Device Has 3 Layers

Application Layer
(Dev Specific)

Network Stack Layer
(Network & Transportation)

Physical Layer
(Link Layer, Chip Layer)



ARMIS

URGENT/11 Enterprise Risk

- Can target a device:
  - On the perimeter of the network
  - Within the network
- In all scenarios
  - Can attack remotely
  - Can gain complete control over the targeted device
  - No user interaction required
  - Can bypass perimeter security and NAT solutions

URGENT/11 Security Advisories

Schneider Electric

Security Bulletin – Wind River VxWorks Vulnerabilities (URGENT/11)

2 August 2019

Overview

Schneider Electric is aware of recently disclosed vulnerabilities in Wind River's VxWorks TCP/IP Stack. These vulnerabilities have wide-ranging impact across multiple IT and industrial applications. We are working closely with Wind River to understand and assess how these vulnerabilities impact Schneider Electric offers and our customers' operations. We downloaded Wind River's patches as soon as they were made available to us, and we have quickly instituted a remediation plan to evolve all current and future products that rely on the Wind River platform to embed these fixes.

We will continue to monitor and will respond further if new information becomes available. In the meantime, customers should immediately make sure they have implemented cybersecurity best practices across their operations to protect themselves from these vulnerabilities. Where appropriate this includes locating your indu… behind firewalls, installing physical controls … mission-critical systems and devices from t…

Please subscribe to the Schneider Electric … updates to this disclosure, including details … as other important security notifications.

https://www.schneider-electric.com/en/work…

For additional information and support, plea… representative or Schneider Electric's Custo…

Details

Additional details on these specific vulnera… notification webpage:

https://www.windriver.com/security/announc…

Of the 11 identified Wind River vulnerabilit… exploitable. Four of those six can be mitigate… to the device is required. The other vulnera… information disclosure.

2-Aug-19 Document Referenc…

Rockwell

Industries Capabilities Products News & Events Sales & Partners Support

VxWorks Vulnerabilities affect
Programmable Automation Controllers, EtherNet/IP Communication Modules, I/O Modules, Kinetix 6500 Servo Drive, High-Frequency RFID Interface Block

Version 1.0 – July 30, 2019

Arms, an IoT security firm, reported a total of eleven vulnerabilities to WindRiver that affect VxWorks, a real-time operating system (RTOS) utilized by many different technology vendors, including Rockwell Automation™. These vulnerabilities, if successfully exploited, may result in several impacts ranging from packet information disclosure to allowing a threat actor to execute arbitrary code on the targeted device.

Not every VxWorks vulnerability applies to every impacted product family. Please see the table under Affected Products for a full list of the potentially affected Rockwell Automation products and the corresponding VxWorks vulnerabilities, which are identified by their Common Vulnerabilities and Exposures (CVE) ID.

Currently, Rockwell Automation is working to address these … available. Please subscribe to updates to this advisory and … notified.

Customers using potentially affected products are encourag… these listed below. Additional details relating to the discove…

AFFECTED PRODUCTS

XEROX

xerox

Printers & Supplies Solutions & Services Customer Support Partners

Wind River VXWorks IPnet TCP/IP STACK Vulnerabilities

Name	Wind River VXWorks IPnet TCP/IP STACK Vulnerabilities
Tracking Number	2019-001
First Publish Date	22 Jul 2019
Date of Current Status	22 Jul 2019
Next Planned Update	22 Aug 2019
Description	A number of vulnerabilities in Wind River's VXWorks IPnet TCP/IP Stack implementation have be… hijack existing TCP sess… Service attacks.
What You Need To Know?	Security researchers re… Stack implementation th… existing TCP/IP connec… or force transmittal of in… middle, replay, and othe…

Currently available info… conditions, and NULL-p… or network connectivity … information also sugge… exploitation.

The 11 CVEs that were … 2019-12265. Exploitab…

One of more of these 1…

- All versions of VxW… SR610)
- Older, End-of-Life ve…
- All versions of the d…
- IPnet when sold as …
- The VxWorks bootro…

VXWorks 5.3 through 6…

PHILIPS

Security Advisory & Archive

VxWorks Urgent/11 Advisory (1 August 2019)

Publication Date: August 1, 2019
Update Date: August 2, 2019

Security researchers at Armis have disclosed 11 different zero-day vulnerabilities within Wind River … used in over 2 billion embedded systems that include medical devices, routers, VOIP phones and … The collection of vulnerabilities, which Armis refers to as "Urgent/11," could lead to remote code exe… whole system without interacting with the user. Of the 11 flaws, six are deemed critical. Successful … an unauthorized user to execute arbitrary code on the target system. An unauthorized user could … data; or create new accounts with full user rights.

Philips is currently monitoring developments and updates related to the recent published advisories … CVEs as referred to as Urgent/11. In the a… consideration for product evaluation and …

As part of the company's product securit… for potential impacts from these reportec… vulnerabilities and evaluating further act… remediate these vulnerabilities. Philips is …

Philips is committed to ensuring the safe… Philips approved product specifications, … or software to Philips' products (includin… Philips product-specific, verified & valida…

If a product does require operating syste… Customer Services, product-specific serv… delivery platforms such as the Philips InC… contract-entitled customers, licensed res…

Contract-entitled customers may use Phi… information posted. If customers still hav… service support team or regional product …

Begin Update A, August 2, 2019

ARMIS

URGENT/11

Many more impacted

- ABACO Systems
- Alcatel-Lucent
- ABB
- Avaya
- Belden Industrial Devices
- BR Automation
- Dräger
- Extreme Networks
- GE Healthcare
- Honeywell
- NetApp
- Opto22
- Philips
- Rockwell Automation
- Schneider Electric
- Siemens
- Spacelabs
- Sonicwall Firewalls
- Trend Micro
- Woodward
- Xerox Printers
- Xylem
- …

URGENT/11

On The Way To Black Hat and DefCon

ARMIS

URGENT/11 BD Alaris tagged as “IPnet"

Alaris PCU

MAC Address:
IPv4 Address:
Manufacturer: Becton Dickinson
Model: Alaris PCU

Category: Medical Therapeutic
Type: Acute Cares
OS: Enea OSE

First Seen At: May 16, 2019 1:43 AM
Last Seen At: Sep 26, 2019 12:14 AM
Last Seen By:

1 Alerts
9 High

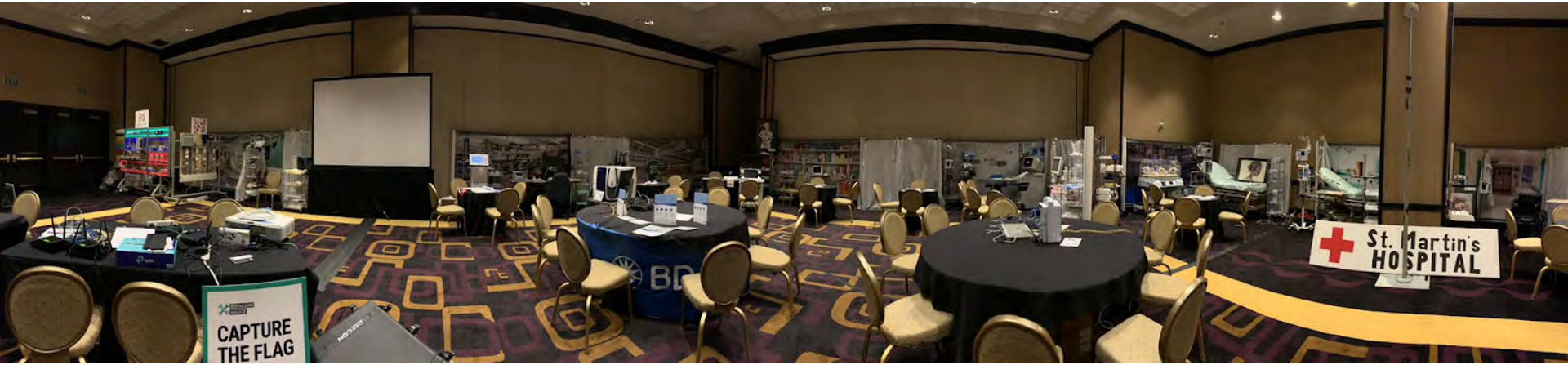
Tags: Corporate × Medical × FDA × IPnet TCP/IP Stack × Add Tag

Device... Connections ... Alert... Activities (... Service... Traffi... Vulnerabiliti... Risk Factor... Enforcement... Application...

URGENT/11 Alaris uses IPnet -> OSE might be impacted

URGENT/**11**

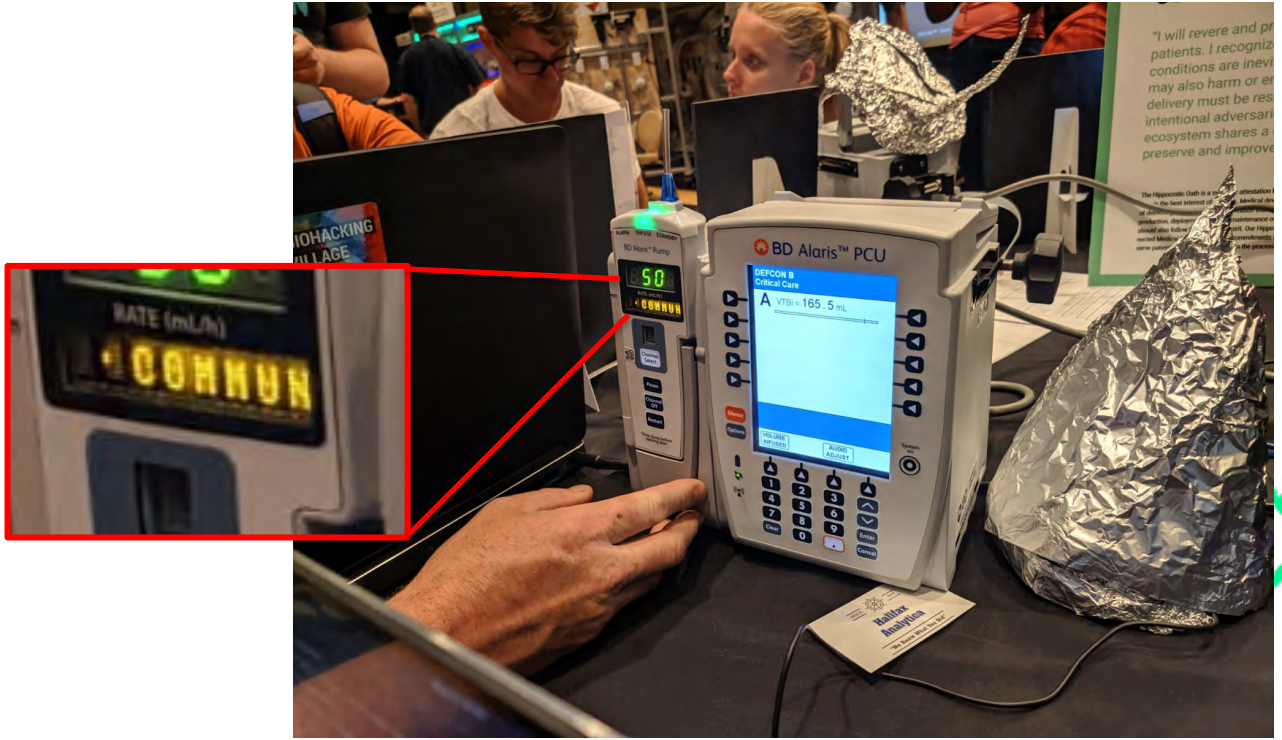
On The Floor of DefCon



BIOHACKING VILLAGE

ARMIS

URGENT/11 COMMUNICATION ERROR



BIOHACKING VILLAGE

ARMIS

URGENT/11 Expanded IPnet Impact

- OSE by ENEA (new)
- Integrity by Green Hills (new)
- ThreadX by Microsoft (new)
- Nucleus RTOS by Mentor (new)
- ITRON by TRON Forum (new)
- ZebOS by IP Infusion (new)

URGENT/11 Cybersecurity Vulnerabilities in a Widely-Used Third-Party Software Component May Introduce Risks During Use of Certain Medical Devices: FDA Safety Communication

Safety Communications

2019 Safety Communications

2018 Safety Communications

2017 Safety Communications

Date Issued: October 1, 2019

The U.S. Food and Drug Administration (FDA) is informing patients, health care providers and facility staff, and manufacturers about cybersecurity vulnerabilities that may introduce risks for certain medical devices and hospital networks. The FDA is not aware of any confirmed adverse events related to these vulnerabilities. However, software to exploit these vulnerabilities is already publicly available.

A security firm has identified 11 vulnerabilities, named "URGENT/11." These vulnerabilities may allow anyone to remotely take control of the medical device and change its function, cause denial of service, or cause information leaks or logical flaws, which may prevent device function.

These vulnerabilities exist in IPnet, a third-party software component that supports network communications between computers. Though the IPnet software may no longer be supported by the original software vendor, some manufacturers have a license that allows them to continue to use it without support. Therefore, the software may be incorporated into other software applications, equipment, and systems which may be used

Content current as of:
10/01/2019

Regulated Product(s)
Medical Devices

URGENT/11 CVEs

CVEs	VxWorks IPnet	Additional RTOSs IPnet
CVE-2019-12256	X	
CVE-2019-12255	X	X
CVE-2019-12260	X	
CVE-2019-12261	X	
CVE-2019-12263	X	
CVE-2019-12257	X	
CVE-2019-12258	X	X
CVE-2019-12262	X	X
CVE-2019-12264	X	X
CVE-2019-12259	X	X
CVE-2019-12265	X	

ARMIS™

URGENT/11 Mitigating the risk

- Identifying vulnerable devices
- Patching if possible
- Preventing an attack using IDS and Firewalls
- Limiting the exposure using network segmentation

URGENT/11 Mitigating the risk

Identifying vulnerable devices:

- Track the advisories published by vendors (through CISA)
- Use Urgent11-Detector tool to actively test devices
- Use passive detection tools for a widescale & permanent solution

URGENT/11 Mitigating the risk

Patching

- Eliminates the risk, but will take the longest time to get done
- Requires a manual process, requires talking devices offline
- Some devices will never get patched

URGENT/11 Mitigating the risk

Preventing an attack using IDS and Firewalls

- Attacks exploiting URGENT/11 will leverage distinct fields in TCP/IP
- IDS rules (Snort) published by Armis

URGENT/11 Signature

The most severe URGENT/11 vulnerabilities abuse esoteric parts of the TCP/IP stack that are almost never used by legitimate applications. Armis has developed the following Snort rules to be freely used by Firewall and IDS solutions to detect and prevent any attempt to exploit these vulnerabilities:

1. Detection of **any** use of the Urgent pointer can be done with the following Snort rule. Be advised that this rule might cause some false positives in the very rare case when Urgent Pointer is used by a legitimate application (such as the ancient RLOGIN protocol).
```
alert tcp any any -> any any (flags: U+; msg: "OS-VXWORKS - Use of Urgent Flag might indicate potential
attempt to exploit an Urgent11 RCE vulnerability"; classtype:attempted-admin; reference:cve,2019-12255;
reference:cve,2019-12260; reference:cve,2019-12261; reference:cve,2019-12263;
reference:url,armis.com/urgent11; rev: 1; sid:1000002)
```
2. Detection of packets that contain both SYN, URG and FIN flags. This combination will never occur in legitimate TCP traffic, and is a strong indication of potential exploit attempt of URGENT/11:
```
alert tcp any any -> any any (flags: SUF+; msg: "OS-VXWORKS Illegal use of Urgent pointer - Potential
attempt to exploit an Urgent11 RCE vulnerability"; classtype:attempted-admin; reference:cve,2019-12255;
reference:cve,2019-12260; reference:cve,2019-12261; reference:cve,2019-12263;
reference:url,armis.com/urgent11; rev: 1; sid:1000001)
```
3. Detection of any IP packet that contains the LSRR or SSRR options. These options should never be used in modern networks, regardless of the potential RCE vulnerability they present to VxWorks devices. Most firewalls will drop any IP packet that contain these packets for security reasons, and IDS solutions can detect any use of such packets using the following Snort rules:
```
alert ip any any -> any any (ipopts: lsrr; msg: "OS-VXWORKS Use of LSRR option, potential attempt to
exploit an Urgent11 RCE vulnerability"; reference:cve,2019-12256; classtype:attempted-admin;
reference:url,armis.com/urgent11; rev: 1; sid:1000003)

alert ip any any -> any any (ipopts: ssrr; msg: "OS-VXWORKS Use of SSRR option, potential attempt to
exploit an Urgent11 RCE vulnerability"; reference:cve,2019-12256; classtype:attempted-admin;
reference:url,armis.com/urgent11; rev: 1; sid:1000004)
```

“We can’t stop everything. So we must find it faster. Our industry is moving to detection and response.”

ACCE Panelist

ARMIS

Agentless Device Security Platform

Discover

- Managed/unmanaged devices
- Wired and wireless
- Risks and vulnerabilities

Analyze

- Behavioral analysis
- Threat detection
- Policy violations

Protect

- Remove suspicious devices
- Manually or per policy
- Inform firewall, SIEM, etc.

NO AGENT / PASSIVE

FRICTIONLESS

ORACLE · Mondelēz International · Allergan · Sysco · MATTRESSFIRM · SAMSUNG

URGENT/11 Resources

Patches

windriver.com/security

Report

armis.com/urgent11

FDA & DHS Advisories

https://www.fda.gov/medical-devices/safety-communications/2019-safety-communications

https://www.us-cert.gov/ics/advisories/icsma-19-274-01

ARMIS

THANK YOU

security@armis.com