WIND RIVER TCP/IP STACK (IPNET) VULNERABILITIES FAQ

BACKGROUND

- A set of vulnerabilities, dubbed "Urgent/11," specific to Wind River's TCP/IP stack (IPnet) were discovered by security company Armis
- The vulnerabilities impact connected devices leveraging VxWorks versions that include the IPnet networking stack
- The latest release of VxWorks is not affected
- Versions of the product designed for safety certification, such as VxWorks 653 and VxWorks Cert Edition are not affected
- Wind River created and unit tested patches for these vulnerabilities, and the patches, along with mitigation options have been provided to customers
- At this time, we have no indication that the discovered vulnerabilities have been exploited in the wild
- Wind River worked closely with Armis to disclose these vulnerabilities to customers. This shared, collaborative process was designed and executed to help device makers mitigate potential risks to their users.
- As the supplier of the world's most widely used and trusted RTOS, Wind River is in the ranks of leading technology companies that have a responsibility to have a prudent security response process in place. This is one of the many things our customers can rely on us for.

Media Inquiries

Direct inquiries to Wind River Corporate Communications: Jessica Miller (jessica.miller@windriver.com / 510.749.2727) or Jenny Suh (jenny.suh@windriver.com / 510.749.2972)

FAQ

1. What was announced?

- A set of 11 security vulnerabilities specific to Wind River's TCP/IP stack (IPnet) were discovered by security researchers at Armis. These vulnerabilities impact VxWorks. Six of the 11 vulnerabilities are considered critical. Armis has dubbed the vulnerabilities "Urgent/11."

2. Which versions of VxWorks are impacted/not impacted?

- VxWorks versions that include the IPnet stack, including end-of-life versions 6.5-6.9 and VxWorks 7 (SR540 and SR610) are impacted. The vulnerabilities do not affect the most recent release of VxWorks 7 (SR0620), or versions of the product designed for safety certification, such as VxWorks 653 and VxWorks Cert Edition.

3. What types of devices are impacted?

- Connected devices leveraging standard VxWorks releases that include the IPnet stack are impacted by the discovered vulnerabilities. They primarily include enterprise devices located at the perimeter of organizational networks that are internet-facing such as modems, routers, firewalls, and printers, as well as some industrial and medical devices.

4. Do all 11 vulnerabilities apply to all impacted versions?

- No, not all 11 vulnerabilities apply to all impacted versions. Some versions could only be impacted by one.

5. **Are patches available?**

- Yes, Wind River created and unit tested patches for these vulnerabilities, and the patches have been provided to customers, along with other mitigation options. Customers can find patch information in the Wind River Knowledge Library.

6. **Where can I find details about the CVEs and vulnerabilities**

- Details can be found in the Wind River Security Alert.

7. **Are all 11 vulnerabilities Remote Code Execution (RCE) vulnerabilities?**

- No, of the 11 vulnerabilities, six can potentially lead to RCE vulnerabilities; and of those six, four can be mitigated by a simple firewall rule.

8. **Does Wind River have built-in security features to protect against these vulnerabilities?**

- Yes, the following built-in VxWorks security features can be applied to form a robust system and protect against the identified IPnet vulnerabilities:

VxWorks Security Feature	Principle	Category	Implementation
Non-executable stack	Availability	Intrusion Protection	Malicious Software Prevention
Real Time Processes	Confidentiality	Separation	Partitioning
System Call Access control	Availability	Whitelisting	Access Control
Task stack overrun/underrun	Availability	Intrusion Protection	Malicious Software Prevention
Firewall	Availability	Intrusion Protection	Firewall
Deterministic Memory Usage	Availability	Countermeasures	Attestation

9. **What support does Wind River offer for these vulnerabilities?**

- Wind River Standard support and maintenance entitles customers to defect fixes, security notifications, and security fixed on the latest supported releases of Wind River products.
- For customers that have released products that cannot always upgrade to the latest releases, Wind River has several offerings to meet those needs including long-term support and long-term maintenance programs, as well as long-term security services to ensure systems are kept current with the latest security patches, included but not limited to:
    - Integration of new features/functions out of the current product line
    - CVE monitoring and patching
    - Tailored support and maintenance addressing specific items aligned industry/applications needs
- Contact your local Wind River sales representative for more information.

10. **Why weren't the vulnerabilities discovered earlier?**

- It is hard to find vulnerabilities in code, and there are people who will attack the code in ways you didn't anticipate. Further, it is not uncommon for security vulnerabilities to go undetected for many years. There are many examples: Spectre/Meltdown existed in millions of processors from dozens of manufactures and went undetected for a decade; OpenSSL vulnerabilities like Heartbleed existed for many years. The fact is, modern software systems are complex with very rich functionality and large code bases written over many years with a constantly advancing awareness of secure programming and constantly increasing levels of scrutiny.

11. Are these vulnerabilities unique to Wind River software?

- These vulnerabilities are not unique to Wind River software. The IPnet stack was acquired by Wind River through its acquisition of Interpeak in 2006. Prior to the acquisition, the stack was broadly licensed to and deployed by a number of RTOS vendors.