Life Is On Schneider Electric

Schneider Electric Security Bulletin

Wind River VxWorks Vulnerabilities (URGENT/11) V1.2

2 August 2019 (9 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 industrial systems and remotely accessible devices behind firewalls; installing physical controls to prevent unauthorized access; and preventing mission-critical systems and devices from being accessed from outside networks.

Please subscribe to the Schneider Electric security notification service to be informed of updates to this disclosure, including details on affected products and remediation plans, as well as other important security notifications:

https://www.schneider-electric.com/en/work/support/cybersecurity/security-notifications.jsp

For additional information and support, please contact your Schneider Electric sales or service representative or Schneider Electric's Customer Care Center.

Details

Additional details on these specific vulnerabilities can be found on the Wind River security notification webpage:

https://www.windriver.com/security/announcements/tcp-ip-network-stack-ipnet-urgent11/

Of the 11 identified Wind River vulnerabilities, six have the potential to trigger remote code execution. Four of those six can be mitigated by a specific firewall configuration, even if access to the device is required. The other vulnerabilities can trigger denial of service conditions or information disclosure.

From the Wind River security alert:

> "*Important to note, not all vulnerabilities apply to all impacted versions. To date, there is no indication the Urgent/11 vulnerabilities have been exploited in the wild.*"

Remediation and Mitigation

Remediating these vulnerabilities requires Schneider Electric to update affected products' firmware. Customers cannot directly apply Wind River patches.

We have downloaded Wind River's patches and are establishing a remediation plan to ensure all current and future Schneider Electric products that rely on the Wind River platform evolve with these embedded fixes.

However, integrating and validating Wind River's patches requires thorough testing and possibly recertification to ensure the quality of the updated product. Therefore, Schneider Electric will update this document once a remediation plan is available. To ensure you are informed of all updates, including details on affected products and remediation plans, please subscribe to Schneider Electric's security notification service:

https://www.schneider-electric.com/en/work/support/cybersecurity/security-notifications.jsp

In the meantime, since the vulnerabilities are present in the TCP/IP stack of the VxWorks product, an active network connection is required to exploit them. Therefore, Schneider Electric customers can act now to mitigate the risk of attack by limiting access to their devices, which would immediately reduce attempted exploits:

- Place Schneider Electric devices in a network with limited access, which will limit their exposure to any attempts to exploit these vulnerabilities.
- Do not expose Schneider Electric devices directly to the internet.
- The impact of these vulnerabilities can be greatly reduced by restricting external network connectivity to the affected devices. Therefore, always place Schneider Electric devices behind firewalls and/or other security protection appliances that limit access only to authorized remote connections.
- Continually monitor affected devices for security events that could warn of attempted unauthorized access.
- Limit access to internal networks where devices reside, which can additionally reduce attempts to exploit these vulnerabilities.

For more details and assistance on how to protect your installation, please contact your local Schneider Electric's Industrial Cybersecurity Services organization, which is fully aware of this situation and can support you through the process.

Affected Products

Industrial Automation Products	Affected Version
ConneXium Industrial Firewalls/Routers	All versions
E+PLC100 Combination PLC	All versions
E+PLC400 Combination PLC	All versions
Magelis HMI - HMIGTO Series, HMISCU Series, HMIGXU Series, HMIGTUX Series, and HMIGTU Series (Except Open BOX)	All versions
Modicon LMC078 Controller	All versions
Modicon M241 Micro PLC	All versions
Modicon M251 Micro PLC	All versions
Modicon M262 Logic/Motion Controller	All versions
Modicon M580 ePAC including Safety CPUs	All versions
Modicon M580 Ethernet / Serial RTU Module	All versions
Modicon M580 Ethernet Communications Modules	All versions
Modicon MC80 Programmable Logic Controller	All versions
Modicon Momentum	All versions
Modicon Quantum 140 CRA	All versions
Modicon Quantum 140 NOP Communications Module	All versions
Modicon X80 I/O Drop Adapters	All versions
Nanodac Recorder / Controller	All versions
PacDrive 3 Eco/Pro/Pro2 Motion Controllers	All versions
Proface HMI - GP4000H/R/E Series, GP4100 Compact Series, LT4000M Modular Series, GP4000E Series, IoT Gateway, SP5000 Series, and SP5000X Series	All versions
SCADAPack 53xE RTUs	All versions
SCADAPack 57x RTUs	All versions
SCD6000 Industrial RTU	All versions
TMSES4 Ethernet Module	All versions
Tricon Communication Modules	TCM/TCM2 V11.1 - V11.4
Trident Communication Integration Module	V3.0
Versadac Scalable Data Recorder	All versions

Energy Management Products	Affected Version
Easergy Micom C264	All versions
Easergy Micom P30	All versions
Easergy Micom P40	All versions
Easergy P5	All versions
Easergy T300 (SC150 & LV150)	All versions
ION7400	All versions
ION7400 MID	All versions
ION9000	All versions

PM8000	All versions
PM8000 MID	All versions
SAGE RTU	All versions
Saitel DR with HU_A CPU only.	All versions
TeSys island Ethernet communication interfaces	All versions

Additional Security Recommendations

We also strongly recommend applying the following industry cybersecurity best practices:

- Locate control and safety system networks and remote devices behind firewalls, and isolate them from the business network.
- Physical controls should be in place so that no unauthorized person would have access to the ICS and safety controllers, peripheral equipment or the ICS and safety networks.
- All controllers should reside in locked cabinets and never be left in the “Program” mode.
- All programming software should be kept in locked cabinets and should never be connected to any network other than the network for the devices that it is intended.
- All methods of mobile data exchange with the isolated network such as CDs, USB drives, etc. should be scanned before use in the terminals or any node connected to these networks.
- Laptops that have connected to any other network besides the intended network should never be allowed to connect to the safety or control networks without proper sanitation.
- Minimize network exposure for all control system devices and/or systems, and ensure that they are not accessible from the Internet.
- When remote access is required, use secure methods, such as Virtual Private Networks (VPNs), recognizing that VPNs may have vulnerabilities and should be updated to the most current version available. Also recognize that VPN is only as secure as the connected devices.

For More Information

This document provides an overview of recently disclosed Wind River VxWorks vulnerabilities and actions required to mitigate them.

For more details and assistance on how to protect your installation, please contact your local Schneider Electric representative and/or Schneider Electric Industrial Cybersecurity Services. These organizations will be fully aware of this situation and can support you through the process.

Schneider Electric Security Bulletin

http://www2.schneider-electric.com/sites/corporate/en/support/cybersecurity/cybersecurity.page

https://www.schneider-electric.com/en/work/services/field-services/industrial-automation/industrial-cybersecurity/industrial-cybersecurity.jsp

Legal Disclaimer

About Schneider Electric

At Schneider, we believe **access to energy and digital** is a basic human right. We empower all to **do more with less**, ensuring **Life Is On** everywhere, for everyone, at every moment.

We provide **energy and automation digital** solutions for **efficiency and sustainability.** We combine world-leading energy technologies, real-time automation, software and services into integrated solutions for Homes, Buildings, Data Centers, Infrastructure and Industries.

We are committed to unleash the infinite possibilities of an **open, global, innovative community** that is passionate with our **Meaningful Purpose, Inclusive and Empowered** values.

www.se.com

Revision Control:

Version 1 *2-Aug-2019*	Original Release
Version 1.1 *7-Aug-2019*	Added Modicon LMC078 Controller to list of affected products, and removed a duplicate product (page 3)
Version 1.1 *9-Aug-2019*	Added SAGE RTU to list of affected products (page 4)

Product Security Office

Digitally signed by Product Security Office
Date: 2019.08.13 19:08:14 -04'00'