PRODUCT CYBERSECURITY NOTIFICATION

Wind River VxWorks Vulnerabilities: Xylem Customer Advisory

Release date: 14 August 2019

Update date: 28 August 2019

Overview

As you may be aware, there was a recent disclosure regarding vulnerabilities in certain versions of Wind River's VxWorks TCP/IP Stack. VxWorks software is a real-time operating system (RTOS) used in many IT and industrial applications. Wind River's disclosure about VxWorks vulnerabilities can be found on the company's security notification webpage, here.

Xylem is evaluating this issue in relation to Xylem products that may have been deployed with components running the vulnerable VxWorks software versions. Based on our investigation to date, we believe the scope of affected Xylem products is narrow.

Xylem's investigation is on-going, however we are already working with the OEM providers of components running VxWorks – including B&R Automation, Rockwell Automation, ABB, Siemens, Schneider Electric, and others – to assess how the recently disclosed vulnerabilities might affect any Xylem products deployed with the software. We will continue to monitor the situation and issue updates and guidance as they become available.

Affected Products

At this time, we believe the potentially affected products are limited to those specified below. If you have any of these products, please review the recommended cybersecurity best practices (below) to help protect them from possible exploitation of the Wind River vulnerabilities.

Product Family	Products	Affected Models	Affected Regions
Bell & Gossett PPS	Parallel Pumping System (PPS) Control Panel - 575V	P2003608	Americas
Bell & Gossett PPS	Parallel Pumping System (PPS) Control Panel - 460V	P2003607	Americas
Bell & Gossett PPS	Parallel Pumping System (PPS) Control Panel - 208/230V	P2003606	Americas
Bell & Gossett PPS	Parallel Pumping System (PPS) Control Panel - 120V	P2003605	Americas
~~Bell & Gossett Technoforce~~	~~DUP, DUAL, TRI, QUAD series boosters~~	~~All models~~	
Bell & Gossett / Goulds Water Technology / Centripro eMT	DUP, DUAL, TRI, QUAD series boosters	All models	Americas
~~Goulds Water Technology / Centripro Aquaforce~~	~~DUP, DUAL, TRI, QUAD series boosters~~	~~All models~~	
Leopold	Engineered to order (ETO) solutions	Including an impacted OEM PLC	Global
Sanitaire	Engineered to order (ETO) solutions	Including an impacted OEM PLC	Global
Wedeco UV	Engineered to order (ETO) solutions	Including an impacted OEM PLC	Global
Wedeco Ozone	Engineered to order (ETO) solutions	Including an impacted OEM PLC	Global

Bell & Gossett / Lowara	Sensorless packages, 2nd water boosters, booster packages	M241 PLC & GXU Touch Panel	China
Lowara	Booster packages	M218 PLC	China
Flygt	TOP / TOP Gate	M241 PLC & GXU Touch Panel	China
Flygt	**Aquaculture Engineered to order (ETO) solutions**	**Including an impacted OEM PLC**	Norway
Flygt	**Transport Engineered to order (ETO) solutions**	**Including an impacted OEM PLC**	Americas

Products added to the list in this update are highlighted in **bold**.

Products determined not to be impacted are marked with a ~~strikethrough~~.

Mitigation Factors and Recommended User Actions

First and foremost, keep in-mind that it is quite straightforward to protect potentially affected devices (Products) against possible exploits. Exploiting the software's vulnerabilities requires an active network connection, so Xylem customers can do the following, now, to mitigate risk:

- Place the Products in a network with limited access, which will limit their exposure to any attempts to exploit these vulnerabilities.
- Do not expose the Products directly to the internet.
- Restrict external network connectivity to the Products.
- Isolate industrial devices (like the Products) to a separate network from non-industrial devices such as users' machines, servers, and printers.
- If you have made modifications to the initial Xylem deployment, please contact us for assistance at product.security@xyleminc.com.
- Continually monitor the Products for security events that could warn of attempted unauthorized access.
- Use trusted software, software patches, anti-virus programs and interact only with trusted websites and attachments. Block all non-trusted IP communications.

Ultimately, determining whether a product is affected and needs remediation requires verification of the VxWorks RTOS version. This requires validation from the OEM.

Additionally, while Wind River's site indicates patches will be available, customers cannot directly apply them. These updates must be incorporated into an OEM patch, and provided by the OEM. Further, integrating and validating these patches requires testing and possibly recertification to ensure the quality of the updated Product.

As remediation paths for the Products become available, we will issue updated guidance.

Support

For support, or with questions about whether specific products may contain the Wind River vulnerabilities, please contact product.security@xyleminc.com.

For further information on industrial network security, refer to https://www.us-cert.gov/ics/Recommended-Practices

For more information on Xylem product security please visit xylem.com/security.