Potential Vulnerabilities
XP503

Date:	12.12.2018
Subject:	Potential Vulnerabilities within XP503
Severity rating:	Medium
Product:	XP503

General Information

Eaton performs regular cybersecurity assessments of our applications and implements improvements to security vulnerabilities identified.

Based on these assessments, Eaton is aware of potential vulnerabilities in XP 503 due to the use of Windows Embedded Standard 7 as the operating system.

The following variants of XP 503 may be affected: XP503 Visual Designer and XP503 Galileo.

A new version of XP 503, for both variants, is scheduled for release in the first quarter of 2019, and customers will be notified of this release.

For additional information or a list of other issues that have been reported and resolved, please visit our Cybersecurity web site www.eaton.com/cybersecurity, or you can contact us at CybersecurityCOE@eaton.com.

Recommendation

In the meantime, Eaton recommends that you follow the best practices listed below, when deploying your product.

Additional guidelines for securely deploying our products are outlined in our whitepaper Cybersecurity considerations for electrical distribution systems.

Best Practices

- *Always install the latest updates from Eaton*
- *Protect access to physical ports and cabinets*
- *Deactivate unused ports/services*
- *Change passwords regularly*
- *Always use least privilege*
- *Whitelist network access if applicable*

Powering Business Worldwide

Eaton
1000 Eaton Boulevard
Cleveland, OH 44122
United States
Eaton.com

Printed in XXX
Publication No. BRXXXXXXXXE / XXX
July 2017