Schneider Electric Security Notification

Foxboro SCADA

13 June 2023

Overview

Schneider Electric is aware of a vulnerability in the AVEVA™ InTouch component which is included as part of the Foxboro SCADA product.

The Foxboro SCADA product is a software package that helps provide SCADA remote communications in the most demanding applications.

Failure to apply the mitigations provided below may allow for the reading of cleartext information stored in memory, which could result in leakage of potentially sensitive data, including password information.

Details

A vulnerability disclosed by AVEVA™ in the InTouch product impacts Schneider Electric Foxboro SCADA products.

Additional information about the vulnerability can be found in the AVEVA Security Bulletin at AVEVA-2021-001.

Affected Products and Versions

Product	Version
Foxboro SCADA	All versions

Mitigations

Affected Product & Version	Mitigations
Foxboro SCADA *All versions*	The Foxboro SCADA product has reached its end of life and is no longer supported. Customers should immediately apply the following mitigations to reduce the risk of exploit: • Hardening access to the engineering workstation and keeping the system up to date • Setting strong user authentication to the operating system to limit access to the memory • Securing storage and removal of memory dump files when no longer required

Schneider Electric Security Notification

General Security Recommendations

We strongly recommend the following industry cybersecurity best practices.

- Locate control and safety system networks and remote devices behind firewalls and isolate them from the business network.
- Install physical controls so no unauthorized personnel can access your industrial control and safety systems, components, peripheral equipment, and networks.
- Place all controllers in locked cabinets and never leave them in the "Program" mode.
- Never connect programming software to any network other than the network intended for that device.
- Scan all methods of mobile data exchange with the isolated network such as CDs, USB drives, etc. before use in the terminals or any node connected to these networks.
- Never allow mobile devices that have connected to any other network besides the intended network to connect to the safety or control networks without proper sanitation.
- Minimize network exposure for all control system devices and 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). Recognize that VPNs may have vulnerabilities and should be updated to the most current version available. Also, understand that VPNs are only as secure as the connected devices.

For more information refer to the Schneider Electric [Recommended Cybersecurity Best Practices](#) document.

For More Information

This document provides an overview of the identified vulnerability or vulnerabilities and actions required to mitigate. For more details and assistance on how to protect your installation, contact your local Schneider Electric representative or Schneider Electric Industrial Cybersecurity Services: https://www.se.com/ww/en/work/solutions/cybersecurity/. These organizations will be fully aware of this situation and can support you through the process.

For further information related to cybersecurity in Schneider Electric's products, visit the company's cybersecurity support portal page: https://www.se.com/ww/en/work/support/cybersecurity/overview.jsp

Schneider Electric Security Notification

About Schneider Electric

Schneider's purpose is to empower all to make the most of our energy and resources, bridging progress and sustainability for all. We call this Life Is On.

Our mission is to be your digital partner for Sustainability and Efficiency.

We drive digital transformation by integrating world-leading process and energy technologies, end-point to cloud connecting products, controls, software and services, across the entire lifecycle, enabling integrated company management, for homes, buildings, data centers, infrastructure and industries.

We are the most local of global companies. We are advocates of open standards and partnership ecosystems that are passionate about our shared Meaningful Purpose, Inclusive and Empowered values.
www.se.com

Revision Control:

Version 1.0 13 June 2023	Original Release