Schneider Electric Security Notification

EcoStruxure™ Foxboro DCS Core Control Services

9 July 2024

Overview

Schneider Electric is aware of multiple vulnerabilities in its EcoStruxure™ Foxboro DCS product.

The EcoStruxure™ Foxboro DCS product is an innovative family of fault-tolerant, highly available control components, which consolidates critical information and elevates staff capabilities to ensure flawless, continuous plant operation.

Failure to apply the remediations provided below may risk local attacks from an authenticated user on the workstation running Foxboro DCS Core Control Services, which could result in loss of system functionality or unauthorized access to system functions.

Affected Products and Versions

Product	Version
EcoStruxure™ Foxboro DCS Core Control Services	Versions 9.8 and prior

Vulnerability Details

CVE ID: **CVE-2024-5679**

CVSS v3.1 Base Score 7.1 | High | CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:H

CWE-787: Out-of-Bounds Write vulnerability exists that could cause local denial-of-service, or kernel memory leak when a malicious actor with local user access crafts a script/program using an IOCTL call in the Foxboro.sys driver.

CVE ID: **CVE-2024-5680**

CVSS v3.1 Base Score 7.1 | High | CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:H

CWE-129: Improper Validation of Array Index vulnerability exists that could cause local denial-of-service when a malicious actor with local user access crafts a script/program using an IOCTL call in the Foxboro.sys driver.

CVE ID: **CVE-2024-5681**

CVSS v3.1 Base Score 7.8 | High | CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

CWE-20: Improper Input Validation vulnerability exists that could cause local denial-of-service, privilege escalation, and potentially kernel execution when a malicious actor with local user access crafts a script/program using an IOCTL call in the Foxboro.sys driver.

Schneider Electric Security Notification

Note regarding vulnerability details: The severity of vulnerabilities was calculated using the CVSS Base metrics in version 3.1 (CVSS v3.1) without incorporating the Temporal and Environmental metrics. Schneider Electric recommends that customers score the CVSS Environmental metrics, which are specific to end-user organizations, and consider factors such as the presence of mitigations in that environment. Environmental metrics may refine the relative severity posed by the vulnerabilities described in this document within a customer's environment.

Remediation

Affected Product & Version	Remediation
EcoStruxure™ Foxboro DCS Core Control Services *v9.8 and prior*	Patch HF97872598 available for v9.5 to v9.8 of EcoStruxure™ Foxboro DCS Core Control Services includes a fix for these vulnerabilities. Please contact your local Service Representative or Schneider Electric Process Automation Global Customer Support Center for information on how to download and install this fix: Process Automation | Global Customer Support (se.com) Reboot is needed.

Customers should use appropriate patching methodologies when applying these patches to their systems. We strongly recommend the use of back-ups and evaluating the impact of these patches in a Test and Development environment or on an offline infrastructure. Contact Schneider Electric's Customer Care Center if you need assistance removing a patch.

If customers choose not to apply the remediation provided above, they should immediately apply the following mitigations to reduce the risk of exploit:

Mitigations

Affected Product & Version	Mitigations
EcoStruxure™ Foxboro DCS Core Control Services *v9.8 and prior*	As the identified vulnerabilities require local user account access, EcoStruxure™ Foxboro DCS workstations should be installed in a secure location to prevent physical access by unauthorized personnel, and appropriate password protections put in place to prevent remote access by unauthorized personnel. To ensure you are informed of all updates, including details on affected products and remediation plans, subscribe to Schneider Electric's security notification service here: https://www.se.com/en/work/support/cybersecurity/security-notifications.jsp

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.

Acknowledgements

Schneider Electric recognizes the following researcher for identifying and helping to coordinate a response to these vulnerabilities:

CVE	Researcher
CVE-2024-5679 CVE-2024-5680 CVE-2024-5681	Vladimir Tokarev, Microsoft Defender for IoT

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.

Schneider Electric Security Notification

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

About Schneider Electric

Schneider's purpose is to **create Impact** by empowering 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 the trusted partner in **Sustainability and Efficiency.**

We are a **global industrial technology leader** bringing world-leading expertise in electrification, automation and digitization to smart **industries**, resilient **infrastructure**, future-proof **data centers**, intelligent **buildings**, and intuitive **homes**. Anchored by our deep domain expertise, we provide integrated end-to-end lifecycle AI enabled Industrial IoT solutions with connected products, automation, software and services, delivering digital twins to enable profitable growth **for our customers.**

We are a **people company** with an ecosystem of 150,000 colleagues and more than a million partners operating in over 100 countries to ensure proximity to our customers and stakeholders. We embrace **diversity and inclusion** in everything we do, guided by our meaningful purpose of a **sustainable future for all**.

www.se.com

Revision Control:

Version 1.0.0 *09 July 2024*	Original Release

CPCERT

Digitally signed by CPCERT
Date: 2024.07.08 13:06:46 -04'00'