Life Is On Schneider Electric

Schneider Electric Security Notification

Andover Continuum Line of Controllers V2.0

12 November 2019 (27 November 2019)

Overview

Schneider Electric is aware of cross-site scripting vulnerability in its line of Andover Continuum building management system controllers. The controllers act as the system coordinators for the Continuum I/O modules, providing integrated global control and monitoring, history logging, local and remote alarming.

Affected Product(s)

Andover Continuum controller models that support the ability to act as their own web server. The Andover continuum controller models that provided built-in web server capability included, but were not limited to, the following models 9680, 5740 and 5720, bCX4040, bCX9640, 9900, 9940, 9924, 9702, and 9200 and 9400 series controllers with the Web Server option enabled.

Vulnerability Details

CVE ID: **CVE-2019-6853**

CVSS v3.0 Base Score 6.1 | (Medium) | CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N

A CWE-79 - A Failure to Preserve Web Page Structure vulnerability exists, which could enable a successful “Cross-site Scripting” (XSS attack) when using the products’ web server.

Remediation

Since Andover Continuum is a legacy product line from which customers have a clear path to our new, state of the art EcoStruxure Building Operation, no firmware fix will be provided for this issue. Rather, the device’s web server should be disabled to reduce risk, using one the methods below:

- Users of the 9680, 5740 and 5720, bCX4040, bCX9640, and 9702 models of network-level controllers should disable the web server by setting the web server port to 0 via the controller web page.
- Users of the 9400, 9410, 9900, 9940 and 9924 models of network controllers should contact the Schneider Electric support group to obtain a unique file that will allow them to disable the controllers’ web servers.

- Compensating controls will be needed to isolate its web browser ports, which would disable the web server. Compensating controls could include incorporating firewalls with access control lists, deep packet inspection and packet filtering.

A controller reboot is required to complete this operation.

Product Information

This notification applies the Andover Continuum line of building controllers.

Product Category - Building and Automation Control

Learn more about Schneider Electric's product categories here: www.schneider-electric.us/en/all-products

How to determine if you are affected

All customers using the identified Continuum controllers are affected.

General Security Recommendations

We strongly recommend following industry cybersecurity best practices, such as:

- 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.

Schneider Electric Security Notification

Acknowledgements

Schneider Electric recognizes the following researcher(s) for identifying and helping to coordinate a response to this vulnerability:

CVE	Researcher(s) Name
CVE-2019-6853	Ken Pyle, DFDR Consulting

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, 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.

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

About Schneider Electric

At Schneider, we believe **access to energy and digital** is a basic human right. We empower all to **make the most of their energy and resources**, 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 about our **Meaningful Purpose, Inclusive and Empowered** values.

www.se.com

Schneider Electric Security Notification

Revision Control:

Version 1.0 *12-Nov-2019*	Original Release
Version 2.0 *27-Nov-2019*	Updated Affected Products and Remediation section.

Product Security Office

Digitally signed by Product Security Office
Date: 2019.11.27 10:57:56 -05'00'