Schneider Electric Security Notification

Andover Continuum System (V2.1)

10 March 2020 (12 May 2020)

Overview

Schneider Electric is aware of multiple vulnerabilities in the Andover Continuum product line. Andover Continuum allows users to view and control functions of the Continuum system.

Affected Product(s)

All Continuum versions are affected.

Vulnerability Details

CVE ID: **CVE-2020-7480**

CVSS v3.0 Base Score 8.8 | High | CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

Continuum XML Vulnerability – The CyberStation product uses the MS-XML version 4.0 library. Issues in this Microsoft functionality may leave CyberStation open to attack.

A CWE-94: Improper Control of Generation of Code ('Code Injection') vulnerability exists which could cause files on the application server filesystem to be viewable when an attacker interferes with an application's processing of XML data.

CVE ID: **CVE-2020-7481**

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

Continuum XSS Vulnerability – The web.Client has a Cross Site Scripting (XSS) vulnerability that may expose the user to various possible attacks.

A CWE-79:Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability exists which could enable a successful “Cross-site Scripting” (XSS attack) when using the products’ web server.

Schneider Electric Security Notification

CVE ID: **CVE-2020-7482**

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

Continuum Reflected XSS Vulnerability – The web.Client has a Reflected Cross Site Scripting (XSS) vulnerability that might allow an attacker to execute unintended code in the context of the user.

A CWE-79:Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability exists which could cause a “Reflective Cross-site Scripting” (XSS attack) when using the products’ web server.

Remediation

Andover Continuum is a classic Schneider Electric product line. New projects are utilizing our more modern, secure and feature rich platform, EcoStruxure Building Operation. For customers with active Continuum installations, Schneider Electric continues to provide resources in a support function where we continue to support the platform per our BMS support policy as these sites work towards transition and modernization to EcoStruxure Building Operation. Given the clear path to EcoStruxure Building Operation and available alternatives to these specific issues, we will not provide a patch for this issue. To reduce risk until modernization to EcoStruxure Building, it is strongly recommended that customers use the methods below:

- It is strongly recommended that the Continuum system be installed on an isolated network segment.
- Compensating controls could include, but not limited to, incorporating firewalls with access control lists, deep packet inspection and packet filtering.

Product Information

The Andover Continuum system allows customers to monitor and maintain building operations.

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 any version of Andover Continuum products.

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 for the devices that it is intended for.
- 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 laptops 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.

Acknowledgements

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

CVE	Researcher(s) Name
CVE-2020-7480, CVE-2020-7481, CVE-2020-7482	Niv Levy from CyberArk Labs

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

Schneider Electric Security Notification

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

Legal Disclaimer

THIS DOCUMENT IS INTENDED TO HELP PROVIDE AN OVERVIEW OF THE IDENTIFIED SITUATION AND SUGGESTED MITIGATION ACTIONS, REMEDIATION, FIX, AND/OR GENERAL SECURITY RECOMMENDATIONS AND IS PROVIDED ON AN "AS-IS" BASIS WITHOUT WARRANTY OF ANY KIND. SCHNEIDER ELECTRIC DISCLAIMS ALL WARRANTIES, EITHER EXPRESS OR IMPLIED, INCLUDING WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. IN NO EVENT SHALL SCHNEIDER ELECTRIC BE LIABLE FOR ANY DAMAGES WHATSOEVER INCLUDING DIRECT, INDIRECT, INCIDENTAL, CONSEQUENTIAL, LOSS OF BUSINESS PROFITS OR SPECIAL DAMAGES, EVEN IF SCHNEIDER ELECTRIC HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THE USE OF THIS NOTIFICATION, INFORMATION CONTAINED HEREIN, OR MATERIALS LINKED TO IT ARE AT YOUR OWN RISK. SCHNEIDER ELECTRIC RESERVES THE RIGHT TO UPDATE OR CHANGE THIS NOTIFICATION AT ANY TIME AND IN ITS SOLE DISCRETION.

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

Revision Control:

Version 1 *10 March 2020*	Original Release
Version 2.0 *14 April 2020*	Revised overview, affected products, vulnerability details, and remediation for clarification (page 1-2)
Version 2.1 *12 May 2020*	Minor updates to overview, vulnerability details, and product information for clarification (page 1-2)

Product Security Office

Digitally signed by Product Security Office
Date: 2020.05.10 20:44:19 -04'00'