Life Is On Schneider Electric

Schneider Electric Security Notification

SoMachine HVAC & SoMove (V2.0)

13 August 2019 (08 October 2019)

Overview

Schneider Electric is aware of a vulnerability in its SoMachine HVAC programming software and SoMove FDT software.

Affected Product(s)

- SoMachine HVAC v2.4.1 and earlier versions
- SoMove FDT v2.7.5 and earlier versions

Vulnerability Details

CVE ID: **CVE-2019-6826**

CVSS v3.0 Base Score 6.8 | (Medium) | CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:H

A CWE-426: Untrusted Search Path vulnerability exists which could cause arbitrary code execution on the system running SoMachine HVAC and SoMove FDT when a malicious DLL library is loaded by the product.

Remediation

This vulnerability is fixed in EcoStruxure Machine Expert HVAC version 1.1.0 (formerly known as SoMachine HVAC) and is available for download below:

https://www.schneider-electric.com/en/download/document/SoMachine%20HVAC%20-%20Programming%20Software%20for%20Modicon%20M171-M172%20Logic%20Controllers/

This vulnerability is fixed in SoMove FDT version 2.7.6 and is available for download below:

https://www.schneider-electric.com/en/download/document/SoMove_FDT/

Schneider Electric Security Notification

Product Information

SoMachine HVAC / EcoStruxure Machine Expert - HVAC is software used for programming Modicon M171-M172 logic controllers.

The SoMove FDT application is used to configure variable speed drives. It requires the installation DTM software components to support the different types of variable speed drives.

Product Category - All Categories

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

How to determine if you are affected

SoMachine HVAC v2.4.1 and prior versions.
Note: The version of SoMachine HVAC is displayed in the title bar of the application or through the About link in the Help menu.

SoMove FDT v2.7.5 and prior versions.
Note: The version of SoMove DTM is displayed in the homepage.

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-2019-6826	Yongjun Liu (nsfocus security team)

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 **do more with less**, 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 with our **Meaningful Purpose, Inclusive and Empowered** values.

www.se.com

Schneider Electric Security Notification

Revision Control:

Version 1 *13 Aug 2019*	Original Release
Version 2.0 *08 Oct 2019*	Added SoMove FDT to the list of affected products (page 1)

Product Security Office

Digitally signed by Product Security Office
Date: 2019.10.07 08:45:15 -04'00'