Schneider Electric Security Notification

SoMachine Basic (V2.0)

18 May 2018 (13 April 2021)

Overview

Schneider Electric has become aware of a vulnerability in the SoMachine Basic (now EcoStruxure Machine Expert - Basic) product.

April 2021 Update: SoMachine Basic has been replaced by EcoStruxure Machine Expert - Basic. Remediation section updated.

Affected Product and Versions

All versions of SoMachine Basic prior to V1.6 SP1

Vulnerability Details

CVE ID: **CVE-2018-7783**

CVSS v3.0 Base Score 8.6 | High | CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H

Schneider Electric SoMachine Basic prior to v1.6 SP1 suffers from an XML External Entity (XXE) vulnerability using the DTD parameter entities technique resulting in disclosure and retrieval of arbitrary data on the affected node via out-of-band (OOB) attack. The vulnerability is triggered when input passed to the xml parser is not sanitized while parsing the xml project/template file.

Remediation

The following steps are required to fix the issue. Please note that SoMachine Basic has been replaced by EcoStruxure Machine Expert - Basic.

STEP 1: Update software and firmware

- On the engineering workstation, update to EcoStruxure Machine Expert - Basic V1.1 SP1 or above: https://www.se.com/ww/en/download/document/Machine_Expert_Basic/
- On Modicon M100/M200/M221 Logic controllers, update to latest firmware version.

STEP 2: Update projects in EcoStruxure Machine Expert – Basic.

- Upgrade the functional level of the application to minimum version 10.2
- Activate the application protection for both read and write in the project properties

STEP 3: Transfer applications.

- Transfer applications to Modicon M100/M200/M221 logic controllers. EcoStruxure Machine Expert – Basic will perform an integrity check when transferring the application and will display a warning pop-up to the user if the application has been altered during transfer

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 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 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 this vulnerability:

CVE	Researchers
CVE-2018-7783	Gjoko Krstikj of Applied Risk

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

LEGAL DISCLAIMER

THIS NOTIFICATION DOCUMENT, THE INFORMATION CONTAINED HEREIN, AND ANY MATERIALS LINKED FROM IT (COLLECTIVELY, THIS "NOTIFICATION") ARE 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 OR GUARANTEE OF ANY KIND. SCHNEIDER ELECTRIC DISCLAIMS ALL WARRANTIES RELATING TO THIS NOTIFICATION, EITHER EXPRESS OR IMPLIED, INCLUDING WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. SCHNEIDER ELECTRIC MAKES NO WARRANTY THAT THE NOTIFICATION WILL RESOLVE THE IDENTIFIED SITUATION. IN NO EVENT SHALL SCHNEIDER ELECTRIC BE LIABLE FOR ANY DAMAGES OR LOSSES WHATSOEVER IN CONNECTION WITH THIS NOTIFICATION, 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. YOUR USE OF THIS NOTIFICATION IS AT YOUR OWN RISK, AND YOU ARE SOLELY LIABLE FOR ANY DAMAGES TO YOUR SYSTEMS OR ASSETS OR OTHER LOSSES THAT MAY RESULT FROM YOUR USE OF THIS NOTIFICATION. 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 **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

Revision Control:

Version 1.0 *22 May 2018*	Original Release
Version 2.0 *13 April 2021*	SoMachine Basic has been replaced by EcoStruxure Machine Expert – Basic and the remediation steps have been updated. (page 1)

Product Security Office

Digitally signed by Product Security Office
Date: 2021.04.11 18:24:53 -04'00'