

Schneider Electric Security Notification

Windows Print Spooler embedded in EcoStruxure™ Process Expert

09 November 2021 (08 March 2022)

Overview

Schneider Electric is aware of a vulnerability in its EcoStruxure™ Process Expert product.

The [EcoStruxure™ Process Expert DCS](#) is a single automation system to engineer, operate, and maintain your entire infrastructure for a sustainable, productive and market-agile plant.

CVE-2021-34527 and CVE-2021-1675, also known as PrintNightmare, affects a native, built-in Windows service named “Print Spooler” that is enabled by default on Windows machines. The purpose of Print Spooler is to manage printers or printer servers.

EcoStruxure™ Process Expert uses Microsoft embedded virtualization technology that cannot be patched using standard Microsoft update steps. An upcoming release of EcoStruxure™ Process Expert will address this issue directly.

Failure to apply the mitigations provided below may allow an attacker to perform privileged file operations, which could result in remote code execution.

March 2022 Update: EcoStruxure™ Process Expert 2021 includes a fix for these vulnerabilities.

Affected Product and Versions

Product	Version
EcoStruxure™ Process Expert	All versions prior to V2021

Vulnerability Details

CVE ID: [CVE-2021-34527](#)

CVSS v3.1 Base Score 8.8 | High | CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Windows Print Spooler Remote Code Execution Vulnerability.

CVE ID: [CVE-2021-1675](#)

CVSS v3.1 Base Score 8.8 | High | CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

Windows Print Spooler Elevation of Privilege Vulnerability.

Schneider Electric Security Notification

Remediations and Mitigations

Affected Product & Version	Remediations and Mitigations
<p>EcoStruxure™ Process Expert</p> <p><i>All versions prior to V2021</i></p>	<p>Version 2021 of EcoStruxure™ Process Expert includes a fix for these vulnerabilities and is available for download here:</p> <p>https://www.se.com/myschneider/documentsDownloadCenterDetail/in/en/EPE2021Release</p> <p>It is recommended to first read the ReadMe in its entirety before proceeding with the software installation.</p> <p>If customers choose not to apply the remediation provided above, they should immediately apply the following mitigations to reduce the risk of exploit:</p> <ul style="list-style-type: none"> • Setup network segmentation and implement a perimeter firewall to filter all unauthorized access to RPC Endpoint Mapper (135/TCP) and SMB (139/TCP and 445/TCP). • Disable the Print Spooler services when print functionality is not needed on all client machines that are authorized to interact with the EPE system server. Please refer to Microsoft Workaround https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34527 • Harden all Windows workstations using the hardening recommendations found in the Cybersecurity Reference Manual <p>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</p>

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.

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.

Schneider Electric Security Notification

- 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.

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.

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

Schneider Electric Security Notification

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 <i>09 November 2021</i>	Original Release
Version 2.0 <i>08 March 2022</i>	EcoStruxure™ Process Expert 2021 includes a fix for these vulnerabilities