

# Schneider Electric Security Notification

## Easy UPS Online Monitoring Software

11 April 2023 (11 June 2024)

### Overview

Schneider Electric is aware of multiple vulnerabilities in its Easy UPS Online Monitoring Software, known as APC Easy UPS Online Monitoring Software, and Schneider Electric UPS Online Monitoring Software known as Schneider SP Series UPS Online Monitoring Software in China.

The Easy UPS Online Monitoring Software is used to configure and manage Easy UPS products.

Failure to apply the remediations provided below may risk remote code execution, escalation of privileges, or authentication bypass, which could result in execution of malicious web code or loss of device functionality.

**June 2024 Update:** Vulnerability description for CVE-2023-29412 has been updated. CWE-78 is correct, but the initial description didn't match with this CWE ID. Remediation instructions were updated to clarify support status.

### Affected Product and Versions

Product	Version
APC Easy UPS Online Monitoring Software	v2.5-GA-01-22320 and prior (Windows 10, 11 Windows Server 2016, 2019, 2022)
Schneider Electric Easy UPS Online Monitoring Software* <i>*Known as Schneider SP Series UPS Monitoring Software in China.</i>	v2.5-GS-01-22320 and prior (Windows 10, 11 Windows Server 2016, 2019, 2022)

# Schneider Electric Security Notification

## Vulnerability Details

CVE ID: **CVE-2023-29411**

CVSS v3.1 Base Score 9.8 | Critical | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

A CWE-306: *Missing Authentication for Critical Function* vulnerability exists that could allow changes to administrative credentials, leading to potential remote code execution without requiring prior authentication on the Java RMI interface.

CVE ID: **CVE-2023-29412**

CVSS v3.1 Base Score 9.8 | Critical | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

CWE-78: *Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')* vulnerability exists that could cause remote code execution when manipulating internal methods through Java RMI interface.

CVE ID: **CVE-2023-29413**

CVSS v3.1 Base Score 7.5 | High | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

CWE-306: *Missing Authentication for Critical Function* vulnerability exists that could cause Denial-of-Service when accessed by an unauthenticated user on the Schneider UPS Monitor service.

*Note regarding vulnerability details: The severity of vulnerabilities was calculated using the CVSS Base metrics in version 3.1 ([CVSS v3.1](#)) without incorporating the Temporal and Environmental metrics. Schneider Electric recommends that customers score the CVSS Environmental metrics, which are specific to end-user organizations, and consider factors such as the presence of mitigations in that environment. Environmental metrics may refine the relative severity posed by the vulnerabilities described in this document within a customer's environment.*

## Schneider Electric Security Notification

### Remediation

Affected Product & Versions	Remediation
<p><b>APC Easy UPS Online Monitoring Software</b> Windows 10, 11 Windows Server 2016, 2019, 2022</p>	<p>Version v2.6-GA-01-23116 of Schneider Electric Easy UPS Online Monitoring Software includes a fix for the vulnerabilities for Microsoft supported versions of Windows (10, 11) and Windows Server (2016, 2019, 2022) and is available for direct download here:  <a href="https://download.schneider-electric.com/files?p_enDocType=Software+-+Release&amp;p_Doc_Ref=APC_install_APC_UPS_windows">https://download.schneider-electric.com/files?p_enDocType=Software+-+Release&amp;p_Doc_Ref=APC_install_APC_UPS_windows</a></p> <p>The Easy UPS Online Monitoring Software has been discontinued coinciding with the discontinuation of the Easy UPS Online SNMP Cards (APV9601, APVS9601) managed by this software.</p> <p>Note: The fix applies to all variants of UPS Online Monitoring Software. It is recommended that customers currently using Easy UPS Online Monitoring Software to manage Easy UPS Online (SRV/SRVS) to transition to PowerChute Serial Shutdown for serial/USB shutdown and monitoring; and to PowerChute Network Shutdown for network shutdown and monitoring. For more information about PowerChute software, please see the following:  <a href="https://www.apc.com/pcss">https://www.apc.com/pcss</a>  <a href="https://www.apc.com/pcns">https://www.apc.com/pcns</a></p>
<p><b>Schneider Electric Easy UPS Online Monitoring Software</b> Windows 10, 11 Windows Server 2016, 2019, 2022*</p> <p><i>*Known as Schneider SP Series UPS Monitoring Software in China.</i></p>	<p>Version v2.6-GS-01-23116 of Schneider Electric Easy UPS Online Monitoring Software includes a fix for the vulnerabilities for Microsoft supported versions of Windows (10, 11) Windows Server (2016, 2019, 2022) and is available for direct download here:  <a href="https://download.schneider-electric.com/files?p_enDocType=Software+-+Release&amp;p_Doc_Ref=APC_install_APC_UPS_windows">https://download.schneider-electric.com/files?p_enDocType=Software+-+Release&amp;p_Doc_Ref=APC_install_APC_UPS_windows</a></p> <p>The Easy UPS Online Monitoring Software has been discontinued coinciding with the discontinuation of the Easy UPS Online SNMP Cards (APV9601, APVS9601) managed by this software.</p> <p>Note: The fix applies to all variants of UPS Online Monitoring Software. It is recommended that customers currently using Easy UPS Online Monitoring Software to manage Easy UPS Online (SRV/SRVS) to transition to PowerChute Serial Shutdown for serial/USB shutdown and monitoring; and to PowerChute Network Shutdown for network shutdown and monitoring. For more information about PowerChute software, please see the following:  <a href="https://www.apc.com/pcss">https://www.apc.com/pcss</a>  <a href="https://www.apc.com/pcns">https://www.apc.com/pcns</a></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

## Schneider Electric Security Notification

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.

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>

If customers choose not to apply the remediation provided above, they should immediately apply the following general security recommendations to reduce the risk of exploit:

### 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.

# Schneider Electric Security Notification

## Acknowledgements

Schneider Electric recognizes the following researchers for identifying and helping to coordinate a response to these vulnerabilities:

CVE	Researchers
CVE-2023-29411	Esjay (@esj4y) working with Trend Micro Zero Day Initiative Nicholas Miles working with Tenable Network Security
CVE-2023-29412 CVE-2023-29413	Esjay (@esj4y) working with Trend Micro Zero Day Initiative

## 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 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

Schneider's purpose is to empower all to make the most of our energy and resources, bridging progress and sustainability for all. We call this Life Is On.

# Schneider Electric Security Notification

Our mission is to be your digital partner for Sustainability and Efficiency.

We drive digital transformation by integrating world-leading process and energy technologies, end-point to cloud connecting products, controls, software and services, across the entire lifecycle, enabling integrated company management, for homes, buildings, data centers, infrastructure and industries.

We are the most local of global companies. We are advocates of open standards and partnership ecosystems that are passionate about our shared Meaningful Purpose, Inclusive and Empowered values.

[www.se.com](http://www.se.com)

## Revision Control:

<b>Version 1.0.0</b> 11 April 2023	Original Release
<b>Version 2.0.0</b> 19 April 2023	The document has been updated to reflect the APC Easy UPS Online Monitoring Software and Schneider Electric Easy UPS Online Monitoring Software remediation is for Windows 10 only. A mitigation for APC Easy UPS Online Monitoring Software and Schneider Electric Easy UPS Online Monitoring Software for Windows 10, 11, Windows Server 2016, 2019, and 2022 has been added.
<b>Version 3.0.0</b> 13 June 2023	A remediation is available that now includes all supported Windows versions.
<b>Version 4.0.0</b> 11 June 2024	Vulnerability description for CVE-2023-29412 has been updated. CWE-78 is correct, but the initial description didn't match with this CWE ID. Remediation instructions were updated to clarify support status.