Schneider Electric Security Notification

Easy UPS Online Monitoring Software

13 December 2022 (11 January 2023)

Overview

Schneider Electric is aware of multiple vulnerabilities in its APC and Schneider Electric branded Easy UPS Online Monitoring Software.

The Easy UPS Online Monitoring Software is used to configure and manage APC and Schneider Electric branded 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.

January 2023 Update: Schneider Electric Easy UPS Online Monitoring Software was added to the list of impacted products, and remediation links were updated.

Affected Product and Versions

Product	Version
APC Easy UPS Online Monitoring Software	V2.5-GA and prior *(Windows 7, 10, 11 Windows Server 2016, 2019, 2022)* V2.5-GA-01-22261 and prior *(Windows 11, Windows Server 2019, 2022)*
Schneider Electric Easy UPS Online Monitoring Software	V2.5-GS and prior *(Windows 7, 10, 11 Windows Server 2016, 2019, 2022)* V2.5-GS-01-22261 and prior *(Windows 11, Windows Server 2019, 2022)*

Vulnerability Details

CVE ID: **CVE-2022-42970**

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

A *CWE-306: Missing Authentication for Critical Function* The software does not perform any authentication for functionality that requires a provable user identity or consumes a significant amount of resources.

CVE ID: **CVE-2022-42971**

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

A *CWE-434: Unrestricted Upload of File with Dangerous Type* vulnerability exists that could cause remote code execution when the attacker uploads a malicious JSP file.

CVE ID: **CVE-2022-42972**

CVSS v3.1 Base Score 7.8 | High | AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

A *CWE-732: Incorrect Permission Assignment for Critical Resource* vulnerability exists that could cause local privilege escalation when a local attacker modifies the webroot directory.

CVE ID: **CVE-2022-42973**

CVSS v3.1 Base Score 7.8 | High | AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

A *CWE-798: Use of Hard-coded Credentials* vulnerability exists that could cause local privilege escalation when local attacker connects to the database.

Remediation

Affected Product & Versions	Remediation
APC Easy UPS Online Monitoring Software *(Windows 7, 10, 11 Windows Server 2016, 2019, 2022)*	Version 2.5-GA-01-22320 of APC Easy UPS Online Monitoring Software includes a fix for the vulnerabilities impacting Windows 7, 10, 11, and Windows Server 2016, 2019, and 2022 and is available for direct download here: https://download.schneider-electric.com/files?p_Doc_Ref=APC_install_APC_UPS_windows&p_enDocType=Software+-+Release&p_File_Name=installAPCUPS_windows-2.5-GA-01-22320.zip
Schneider Electric Easy UPS Online Monitoring Software *(Windows 7, 10, 11 Windows Server 2016, 2019, 2022)*	Version 2.5-GS-01-22320 of Schneider Electric Easy UPS Online Monitoring Software includes a fix for the vulnerabilities impacting Windows 7, 10, 11, and Windows Server 2016, 2019, and 2022 and is available for direct download here: https://download.schneider-electric.com/files?p_Doc_Ref=Install_Schneider_UPS_windows&p_enDocType=Software+-+Release&p_File_Name=installSchneiderUPS_windows.zip

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.

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

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 researchers for identifying and helping to coordinate a response to these vulnerabilities:

CVE	Researchers
CVE-2022-42970 CVE-2022-42971 CVE-2022-42973	rgod working with Trend Micro Zero Day Initiative
CVE-2022-42972	Piotr Bazydlo (@chudypb) of 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.

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

Revision Control:

Version 1.0 *13 December 2022*	Original Release
Version 2.0 *11 January 2023*	Schneider Electric Easy UPS Online Monitoring Software was added to the list of impacted products, and remediation links were updated.

Product Security Office

Digitally signed by Product Security Office
Date: 2023.01.11 12:22:24 -05'00'