Schneider Electric Security Notification

APC by Schneider Electric Rack PDU

14 December 2021(21 December 2021)

Overview

Schneider Electric is aware of a vulnerability in its Rack Power Distribution Unit (PDU) products.

The Rack PDU products (AP7xxxx, AP8xxxx, and APDU9xxx series) are devices that provide real-time remote monitoring at the outlet level to provide:

- advanced data center energy management
- advanced load management
- on/off outlet level power cycling
- sequencing control

Failure to apply the mitigations provided below may risk a cross-site scripting attack, which could result in execution of malicious web code, or unintended device operation.

December 2021 Update: CVSS score updated to 6.5.

Affected Products and Versions

Product	Version
AP7xxxx and AP8xxx with NMC2	V6.9.6 or earlier
AP7xxx and AP8xxx with NMC3	V1.1.0.3 or earlier
APDU9xxx with NMC3	V1.0.0.28 or earlier

Vulnerability Details

CVE ID: **CVE-2021-22825**

CVSS v3.1 Base Score 6.5 | Medium | CVSS:3.1/AV:N/AC:H/PR:L/UI:R/S:C/C:N/I:H/A:L

A *CWE-200: Exposure of Sensitive Information to an Unauthorized Actor* vulnerability exists that could allow an attacker to access the system with elevated privileges when a privileged account clicks on a malicious URL that compromises the security token.

Remediation

Affected Product & Version	Remediation
AP7xxxx and AP8xxx with NMC2	V7.0.6 of the Rack PDU firmware includes a fix for this vulnerability and is available for download here • Rack PDU v7.0.6 firmware here • Device must be rebooted as part of the update process • Verify the firmware version is correct once the update is complete
AP7xxx and AP8xxx with NMC3	V1.2.0.2 of the Rack PDU firmware includes a fix for this vulnerability and is available for download here • Rack PDU v1.2.0.2 firmware here • Release notes here • Device must be rebooted as part of the update process • Verify the firmware version is correct once the update is complete
APDU9xxx with NMC3	V1.2.0.2 of the Rack PDU firmware includes a fix for this vulnerability and is available for download here • Rack PDU v1.2.0.2 firmware here • Release notes here • Device must be rebooted as part of the firmware update process • Verify the firmware version is correct once the update is complete

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.

If customers choose not to apply the remediations provided above, they should immediately apply the following mitigations to reduce the risk of exploit:

- Discontinue the use of outlet links until the firmware upgrade is applied.

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.

Acknowledgement

Schneider Electric recognizes the following researcher for identifying and helping to coordinate a response to this vulnerability:

CVE	Researcher
CVE-2021-22825	Andrea Palanca (Nozomi Networks)

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

Schneider Electric Security Notification

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 *14 December 2021*	Original Release
Version 1.1 *21 December 2021*	CVSS score updated to 6.5.

Product Security Office

Digitally signed by Product Security Office
Date: 2021.12.20 18:32:51 -05'00'