Schneider Electric Security Notification

APC by Schneider Electric Network Management Cards (NMC) and NMC Embedded Devices

09 November 2021 (10 May 2022)

Overview

Schneider Electric is aware of multiple vulnerabilities in its products that use the Network Management Card 2 (NMC2), Network Management Card 3 (NMC3), and the NMC embedded devices.

The NMC2 and the NMC3 cards and embedded devices allow for secure monitoring and control of APC by Schneider Electric products.

Failure to apply the mitigations provided below may risk potential data disclosure or cross-site scripting which could result in execution of malicious web code or loss of device functionality.

May 2022 Update: Remediations added for remaining affected products: APC Power Distribution products (page 4-5), Cooling products (page 6), Environmental Monitoring products (page 7), and Battery Management products (page 7).

Affected Products

Network Management Card 2 (NMC2),Network Management Card 3 (NMC3), and the NMC embedded devices including:

- Uninterruptible Power Supply (UPS) products
- APC Power Distribution products
- Cooling products
- Environmental Monitoring products
- Battery Management products

Specific affected product and version details in the Remediations & Mitigations section below.

Vulnerability Details

CVE ID: **CVE-2021-22810**

CVSS v3.1 Base Score 6.8 Medium | CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:N

A *CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')* vulnerability exists that could cause arbitrary script execution when a privileged account clicks on a malicious URL specifically crafted for the NMC pointing to a delete policy file.

CVE ID: **CVE-2021-22811**

CVSS v3.1 Base Score 6.8 | Medium | CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:N

A *CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')* vulnerability exists that could cause script execution when the request of a privileged account accessing the vulnerable web page is intercepted.

CVE ID: **CVE-2021-22812**

CVSS v3.1 Base Score 6.8 | Medium | CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:N

A *CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')* vulnerability exists that could cause arbitrary script execution when a privileged account clicks on a malicious URL specifically crafted for the NMC.

CVE ID: **CVE-2021-22813**

CVSS v3.1 Base Score 6.8 | Medium | CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:N

A *CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')* vulnerability exists that could cause arbitrary script execution when a privileged account clicks on a malicious URL specifically crafted for the NMC pointing to an edit policy file.

CVE ID: **CVE-2021-22814**

CVSS v3.1 Base Score 6.8 | Medium | CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:N

A *CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')* vulnerability exists which could cause arbitrary script execution when a malicious file is read and displayed.

CVE ID: **CVE-2021-22815**

CVSS v3.1 Base Score 5.3 | Medium | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

A *CWE-200: Information Exposure* vulnerability exists which could cause the troubleshooting archive to be accessed.

Remediations

Product & Affected Versions	Remediations
Uninterruptible Power Supply (UPS) Products	
1-Phase Uninterruptible Power Supply (UPS) using NMC2 including Smart-UPS, Symmetra, and Galaxy 3500 with Network Management Card 2 (NMC2): - AP9630/AP9630CH/AP9630J - AP9631/AP9631CH/AP9631J - AP9635/AP9635J ***Affected Versions - NMC2 AOS V6.9.8 and prior***	V7.0.4 or later of the NMC2 SUMX and SY applications includes fixes for these vulnerabilities and are available for download via the links below: SUMX (SmartUPS & Galaxy 3500) SY (Single Phase Symmetra) SUMX & SY Release notes
3-Phase Uninterruptible Power Supply (UPS) using NMC2 including Symmetra PX 250/500 (SYPX) Network Management Card 2 (NMC2): - AP9630/AP9630CH/AP9630J - AP9631/AP9631CH/AP9631J - AP9635/AP9635J ***Affected Versions - NMC2 AOS V6.9.6 and prior***	V7.0.4 or later of the NMC2 SYPX application includes fixes for these vulnerabilities and has been released. Please contact your local support team for SYPX application upgrade.
3-Phase Uninterruptible Power Supply (UPS) using NMC2 including Symmetra PX 48/96/100/160 kW UPS (PX2), Symmetra PX 20/40 kW UPS (SY3P), Gutor (SXW, GVX), and Galaxy (G300, GVMTS, GVMSA, GVXTS, GVXSA, G7K, GFC, G9KCHU, CHU) - AP9630/AP9630CH/AP9630J - AP9631/AP9631CH/AP9631J - AP9635/AP9635CH ***Affected Versions - NMC2 AOS V6.9.6 and prior***	V7.0.4 or later for the Symmetra PX 48/96/100/160 kW UPS (PX2), Symmetra PX 20/40 kW UPS (SY3P), Gutor (SXW, GVX), and Galaxy (G300, GVMTS, GVMSA, GVXTS, GVXSA, G7K, GFC, G9KCHU, CHU) includes fixes for these vulnerabilities has been released. Please contact your local support team for application upgrades for these models.

1-Phase Uninterruptible Power Supply (UPS) using NMC3 including Smart-UPS, Symmetra, and Galaxy 3500 with Network Management Card 3 (NMC3): • AP9640/AP9640J • AP9641/AP9641J • AP9643/AP9643J ***Affected Versions* – NMC3 AOS V1.4.2.1 and prior**	V1.5 or later of the NMC3 SU and SY applications include fixes for these vulnerabilities and are available for download via the links below: SU (SmartUPS & Galaxy 3500) SY (Single Phase Symmetra) Release Notes
APC Power Distribution Products	
APC Rack Power Distribution Units (PDU) using NMC2 • 2G Metered/Switched Rack PDUs with embedded NMC2: AP84xx, AP86xx, AP88xx, AP89xx ***Affected Versions – NMC2 AOS V6.9.6 and prior***	V7.0.6 or later of the NMC2 RPDU2G application includes fixes for these vulnerabilities and is available for download via the link below: RPDU2G Firmware Release notes
APC Rack Power Distribution Units (PDU) using NMC3 • 2G Metered/Switched Rack PDUs with embedded NMC3: APDU99xx ***Affected Versions – NMC3 AOS V1.4.0 and prior***	NMC3 RPDU application V1.2.0.2 with NMC3 AOS v1.5.0 includes fixes for these vulnerabilities and are available for download via the links below: RPDU2G Firmware Release Notes
APC 3-Phase Power Distribution Products using NMC2 • Galaxy RPP • GRPPIP2X84 ***Affected Versions – NMC2 AOS V6.9.6 and prior***	V7.0.4 or later of the NMC2 RPP application includes fixes for these vulnerabilities and is available for download via the link below. Galaxy RPP Firmware

Network Management Card 2 (NMC2) for InfraStruxure 150 kVA PDU with 84 Poles (X84P) • PDPB150G6F **Network Management Card 2 for InfraStruxure 40/60kVA PDU (XPDU)** • PD40G6FK1-M, PD40F6FK1-M, PD40L6FK1-M, PDRPPNX10 M,PD60G6FK1, PD60F6FK1, PD60L6FK1, PDRPPNX10, PD40E5EK20-M, PD40H5EK20-M **Network Management Card 2 for Modular 150/175kVA PDU (XRDP)** • PDPM150G6F, PDPM150L6F, PDPM175G6H **Network Management Card 2 for 400 and 500 kVA (PMM)** • PMM400-ALA, PMM400-ALAX, PMM400-CUB, PMM500-ALA, PMM500-ALAX, PMM500-CUB **Network Management Card 2 for Modular PDU (XRDP2G)** • PDPM72F-5U, PDPM138H-5U, PDPM144F, PDPM138H-R, PDPM277H, PDPM288G6H ***Affected Versions – NMC2 AOS V6.9.6 and prior***	V7.0.4 or later of the NMC2 for X84P, XPDU, XRDP, PMM, and XRDP2G applications includes fixes for these vulnerabilities. Please contact your local support team for application upgrade.
Rack Automatic Transfer Switches (ATS) Embedded NMC2: • Rack Automatic Transfer Switches - AP44xx (ATS4G) ***Affected Versions – NMC2 AOS V6.9.6 and prior***	V7.0.4 or later of the NMC2 ATS4G application include fixes for these vulnerabilities and are available for download via the link below: ATS4G Firmware

Cooling Products	
Network Management Card 2 (NMC2) Cooling Products • InRow Cooling for series ACRP5xx, ACRP1xx, ACRD5xx, and ACRC5xx SKUs (ACRP2G) • InRow Cooling for series ACRC10x SKUs (RC10X2G) • InRow Cooling for series ACRD6xx and ACRC6xx SKUs (ACRD2G) • InRow Cooling Display for series ACRD3xx (ACRC2G) • InRow Cooling for series ACSC1xx SKUs (SC2G) • InRow Cooling for series ACRD1xx and ACRD2xx (ACRPTK2G) • Ecoflair IAEC25/50 Air Economizer Display (EB2G) • Uniflair SP UCF0481I, UCF0341I (UNFLRSP) • Uniflair AM Perimeter Cooling for SKUs: SDCC, SDCV, SDAC, ADAV, SDWC, SDWV, SUAC, SUAV, SUWC, and SUWV (AMICO) • Uniflair LE DX Perimeter Cooling Display for SKUs: IDAV, IDEV, IDWV, IUAV, IUEV, IUWV, IXAV, IXEV, IXWV, LDAV, LDEV, and LDWV (LEDX2G) • Uniflair LEL Perimeter Cooling for SKUs: LDCV, LUCV (UNFLRLEL) • Uniflair Display for Aquaflair TSA/TRA Chiller (UNFLRTSA) • Uniflair Display for Trim Chiller (TRMCHLR) • Uniflair BCWC Chiller (AQUACENTR) • Refrigerant Distribution Unit: ACDA9xx (RDU) *Affected Versions – NMC2 AOS V6.9.6 and prior*	V7.0.4 or later of the NMC2 of these cooling applications include fixes for these vulnerabilities and have been released. Please contact your local support team for upgrades.

Environmental Monitoring Products	
Environmental Monitoring Unit with embedded NMC2 (NB250) • NetBotz NBRK0250 *Affected Versions – NMC2 AOS V6.9.6 and prior*	V7.0.4 or later of the NMC2 NB250 application includes fixes for these vulnerabilities and has been released. NB250 Firmware
Battery Management Products	
Network Management Card 2 (NMC2) • AP9922 Battery Management System (BM4)	V7.0.4 or later of the NMC2 BM4 application includes fixes for these vulnerabilities and has been released. Please contact your local support team for BM4 application upgrade.
EcoStruxure Micro Data Center • EcoStruxure Micro Data Center (MDC) *Affected Versions – NMC2 AOS V6.9.6 and prior*	V7.0.4 or later of the NMC2 MDC application includes fixes for these vulnerabilities and has been released. Please contact your local support team for MDC application upgrade.

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 remediation provided above, they should immediately apply the following mitigations to reduce the risk of exploit:

- NMC users should not trust links provided from sources which have not been verified as authentic.
- Ensure the workstation where the browser is being used is secured.
- If a debug.tar file is generated via Web or CLI, ensure it is deleted after retrieval.

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.
- 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	Researcher Name
CVE-2021-22810, CVE-2021-22811, CVE-2021-22812, CVE-2021-22813, CVE-2021-22815	Chua Wei Kiat of Fortinet's Fortiguard Labs Thanh Nguyen of Fortinet's Fortiguard Labs
CVE-2021-22814	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

Schneider Electric Security Notification

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 *09 November 2021*	Original Release
Version 2.0 *10 May 2022*	Remediations added for remaining affected products: APC Power Distribution products (page 4-5), Cooling products (page 6), Environmental Monitoring products (page 7), and Battery Management products (page 7).

Product Security Office

Digitally signed by Product Security Office
Date: 2022.05.06 14:24:38 -07'00'