

APC by Schneider Electric Network Management Cards (NMC) and NMC Embedded Devices (V2.3)

22 June 2020 (30 June 2021)

Overview

Schneider Electric became aware of multiple vulnerabilities affecting Treck Inc.'s embedded TCP/IP stack, collectively known as Ripple20, which Treck publicly disclosed on June 16, 2020. Schneider Electric is also aware of a proof of concept published by JSOF that demonstrates how one of the Treck vulnerabilities, CVE-2020-11901, can be exploited to affect a Schneider Electric APC Smart-UPS device using certain Network Management Card firmware versions.

On October 12, 2020, Schneider Electric received additional information and analysis from JSOF related to CVE-2020-11901's impact on APC by Schneider Electric Network Management Cards and NMC embedded devices. This new analysis indicates that the information we originally received was incomplete. Therefore our original remediations are only partially effective for CVE-2020-11901. We are expediting updated remediations, which will be made available as soon as possible. In the meantime, customers should immediately apply the mitigations included in [Remediation & Mitigations](#) section of this document.

June 2021 Update: Added remediations for *Uninterruptible Power Supply (UPS)*, *Rack Power Distribution Units (rPDU)*, *Battery Management*, *Rack Automatic Transfer Switch (ATS)*, *Rack Air Removal Unit (RARU) using NMC1*, as well as all other remaining *NMC1 applications*.

Affected Products & Remediations

Schneider Electric has determined that the offers on the following page are impacted. The company will update this table as it continues to assess the impact these vulnerabilities have on its offers.

Please subscribe to the Schneider Electric security notification service to be informed of critical updates to this notification, including information on affected products and remediation plans:

<https://www.se.com/ww/en/work/support/cybersecurity/security-notifications.jsp>

Available Remediations

Product	Affected Version	Addressed CVEs	Remediation/Mitigation
<p><u>Uninterruptible Power Supply (UPS) using NMC2</u></p> <p>1-Phase and 3-Phase UPS models including Smart-UPS, Symmetra, and Galaxy with Network Management Card 2 (NMC2):</p> <ul style="list-style-type: none"> - AP9630/AP9630CH/AP9630J - AP9631/AP9631CH/AP9631J - AP9635/AP9635CH 	<p>NMC2 AOS V6.9.4 and earlier</p>	<p>All CVEs impacting NMC2*</p> <p><i>*Full list in the Vulnerability Details section</i></p>	<p>Patches for the vulnerabilities have begun being released for applications running on the NMC2 platforms.</p> <p>Customers are urged to upgrade to applications using NMC2 AOS V6.9.6 or later.</p> <p>Note: AOS V6.9.2/6.9.4 addressed 14 of the 15 CVEs. AOS V6.9.6 addresses CVE-2020-11901.</p> <p>Refer to this link for the latest information on application patch availability: https://www.apc.com/us/en/faqs/FA410359/</p>
<p><u>Uninterruptible Power Supply (UPS) using NMC1 - SUMX</u></p> <ul style="list-style-type: none"> - AP9617 (discontinued in Nov 2011) - AP9619 (discontinued in Sep 2012) - AP9618 (discontinued in Jan 2017) - Smart-UPS models embedded with NMC1 	<p>Smart-UPS NMC1 v3.9.2 and earlier</p>	<p>All CVEs impacting NMC1*</p> <p><i>*Full list in the Vulnerability Details section</i></p>	<p>Patches for the vulnerabilities have been released for the SUMX application running on the NMC1 platform.</p> <p>Customers are urged to upgrade to applications using NMC2 AOS V3.9.4 or later.</p> <p>Refer to this link for the latest information on application patch availability: https://www.apc.com/us/en/faqs/FA410359/</p>
<p><u>Uninterruptible Power Supply (UPS) using NMC3</u></p> <p>Network Management Card 3 (NMC3) SmartSlot card models:</p> <ul style="list-style-type: none"> - AP9640/AP9640J - AP9641/AP9641J 	<p>NMC3 AOS V1.3.0.6 and earlier</p>	<p>All CVEs impacting NMC3*</p> <p><i>*Full list in the Vulnerability Details section</i></p>	<p>Patches for the vulnerabilities have begun being released for applications running on the NMC3 platforms.</p> <p>Customers are urged to upgrade to applications using NMC3 AOS V1.4 or later.</p> <p>Note: AOS V1.3.3.1 addressed 14 of the 15 CVEs. NMC3 AOS V1.4 addresses CVE-2020-11901.</p> <p>Refer to this link for the latest information on application patch availability: https://www.apc.com/us/en/faqs/FA410359/</p>

<p><u>Battery Management</u></p> <p>Embedded NMC2</p> <ul style="list-style-type: none"> - Battery Manager - AP9922 	<p>NMC2 AOS V6.9.4 and earlier</p>	<p>All CVEs impacting NMC2*</p> <p><i>*Full list in the Vulnerability Details section</i></p>	<p>Patches for the vulnerabilities have begun being released for applications running on the NMC2 platform.</p> <p>Customers are urged to upgrade to applications using AOSV6.9.6 or later.</p> <p>Note: AOS V6.9.2/6.9.4 addressed 14 of the 15 CVEs. AOS V6.9.6 addresses CVE-2020-11901.</p> <p>Refer to this link for the latest information on application patch availability: https://www.apc.com/us/en/faqs/FA410359/</p>
<p><u>APC 3-Phase Power Distribution Products:</u></p> <ul style="list-style-type: none"> - InfraStruXure 150kVA PDU with 84 poles (X84P) - InfraStruXure 40 and 60 kVA PDU (XPDU) - Modular 150 and 175 kVA PDU NAM (XRDP) - 400 and 500 kVA PMM (PMM) - Modular PDU/RPP (XRDP2G) 	<p>NMC2 AOS V6.9.4 and earlier</p>	<p>All CVEs impacting NMC2*</p> <p><i>*Full list in the Vulnerability Details section</i></p>	<p>Patches for the vulnerabilities have begun being released for applications running on the NMC2 platform.</p> <p>Customers are urged to upgrade to applications using AOSV6.9.6 or later.</p> <p>Note: AOS V6.9.2/6.9.4 addressed 14 of the 15 CVEs. AOS V6.9.6 addresses CVE-2020-11901.</p> <p>Refer to this link for the latest information on application patch availability: https://www.apc.com/us/en/faqs/FA410359/</p>
<p><u>APC Rack Power Distribution Units (rPDU)*</u></p> <p>Embedded NMC2:</p> <ul style="list-style-type: none"> - 2G Metered/Switched Rack PDUs with embedded NMC2 - AP84XX, AP86XX, AP88XX, AP89XX 	<p>NMC2 AOS V6.9.4 and earlier</p>	<p>All CVEs impacting NMC2*</p> <p><i>*Full list in the Vulnerability Details section</i></p>	<p>Patches for the vulnerabilities have been released for applications running on the NMC2 platform.</p> <p>Customers are urged to upgrade to applications using AOSV6.9.6 or later.</p> <p>Note: AOS V6.9.2/6.9.4 addressed 14 of the 15 CVEs. AOS V6.9.6 addresses CVE-2020-11901.</p> <p>Refer to this link for the latest information on application patch availability: https://www.apc.com/us/en/faqs/FA410359/</p>

<p><u>APC Rack Power Distribution Units (rPDU)*</u></p> <p>Embedded NMC1: Metered/Switched Rack PDUs with embedded NMC1 - AP78XX, AP79XX</p>	<p>NMC1 AOS V3.9.2 and earlier</p>	<p>All CVEs impacting NMC1 <i>Full list in the Vulnerability Details section</i></p>	<p>Patches for the vulnerabilities have been released for applications running on the NMC1 platform.</p> <p>Customers are urged to upgrade to applications using NMC1 AOSV3.9.4 or later</p> <p>Refer to this link for the latest information on application patch availability: https://www.apc.com/us/en/faqs/FA410359/</p>
<p><u>Rack Automatic Transfer Switches (ATS)*</u></p> <p>Embedded NMC2: - Rack Automatic Transfer Switches - AP44XX</p> <p>Embedded NMC1: - Rack Automatic Transfer Switches - AP77XX</p>	<p>NMC2 AOS V6.8.8 and earlier</p> <p>NMC1 AOS v3.9.2 and earlier</p>	<p>All CVEs impacting NMC1 and NMC2*</p> <p><i>*Full list in the Vulnerability Details section</i></p>	<p>Patches for the vulnerabilities have been released for applications running on the NMC1 and NMC2 platform.</p> <p>Customers are urged to upgrade to applications using NMC2 AOSV6.9.6 or later or NMC1 AOSv3.9.4 or later</p> <p>Note: NMC2 AOS V6.9.2/6.9.4 addressed 14 of the 15 CVEs. AOS V6.9.6 addresses CVE-2020-11901.</p> <p>Refer to this link for the latest information on application patch availability: https://www.apc.com/us/en/faqs/FA410359/</p>
<p><u>Environmental Monitoring*</u></p> <p>Environmental Monitoring Unit with embedded NMC2 - NetBotz NBRK0250</p>	<p>NMC2 AOS V6.8.8 and earlier</p>	<p>All CVEs impacting NMC2*</p> <p><i>*Full list in the Vulnerability Details section</i></p>	<p>Patches for the vulnerabilities have been released for applications running on the NMC2 platform.</p> <p>Customers are urged to upgrade to applications using AOSV6.9.6 or later.</p> <p>Note: AOS V6.9.2/6.9.4 addressed 14 of the 15 CVEs. AOS V6.9.6 addresses CVE-2020-11901.</p> <p>Refer to this link for the latest information on application patch availability: https://www.apc.com/us/en/faqs/FA410359/</p>

<p><u>Cooling Products*</u></p> <p>Embedded NMC2 & Touchscreen Displays:</p> <ul style="list-style-type: none"> - InRow - Uniflair Cooling Devices 	<p>NMC2 AOS V6.9.4 and earlier</p>	<p>All CVEs impacting NMC2*</p> <p><i>*Full list in the Vulnerability Details section</i></p>	<p>Patches for the vulnerabilities have begun being released for applications running on the NMC2 platform.</p> <p>Customers are urged to upgrade to applications using AOSV6.9.6 or later.</p> <p>Note: AOS V6.9.2/6.9.4 addressed 14 of the 15 CVEs. AOS V6.9.6 addresses CVE-2020-11901.</p> <p>Refer to this link for the latest information on application patch availability: https://www.apc.com/us/en/faqs/FA410359/</p>
<p><u>Cooling Products*</u></p> <p>Embedded NMC1</p> <ul style="list-style-type: none"> - Rack Air Removal Unit SX (RARU) 	<p>NMC1 AOS V3.9.2 and earlier</p>	<p>All CVEs impacting NMC1*</p> <p><i>*Full list in the Vulnerability Details section</i></p>	<p>Patches for the vulnerabilities have been released for RARU NMC1 application</p> <p>Customers are urged to upgrade to applications using NMC1 AOSV3.9.4 or later</p> <p>Refer to this link for the latest information on application patch availability: https://www.apc.com/us/en/faqs/FA410359/</p>

<p><u>NMC1 Products</u></p> <p>Symmetra UPS Network Management Card 1 (NMC1) SmartSlot Models:</p> <ul style="list-style-type: none"> - AP9617 (discontinued in Nov 2011) - AP9619 (discontinued in Sep 2012) - AP9618 (discontinued in Jan 2017) - Audio/Video Network Management Enabled products S20BLK, G50NETB2, G50NETB-20A2 <p>Battery Management</p> <ul style="list-style-type: none"> - Battery Management System - AP9920B1 - Battery Management System - AP9921X <p>Environmental Monitoring Units</p> <ul style="list-style-type: none"> - AP9319 - AP9320 - AP9340 - AP9360 - AP9361 - NetBotz NBRK0200 <p>Cooling Products</p> <ul style="list-style-type: none"> - NetworkAir - InRow 	<p>NMC1 AOS V3.9.2 and earlier</p>	<p>All CVEs impacting NMC1*</p> <p><i>*Full list in the Vulnerability Details section</i></p>	<p>These are End of Commercialization offers.</p> <p>To reduce risk of exploitation, apply the mitigations detailed in the Recommended Mitigations section.</p> <p>Contact your local support team for further assistance in upgrading to NMC2 or NMC3 platforms.</p>
--	--	---	---

Mitigations

Schneider Electric is implementing remediations which will be made available as soon as possible. In the meantime, we recommend that our customers protect their installations from the cyber risks associated with the Treck vulnerabilities by immediately taking these mitigating actions:

For devices on a local network:

- Network Partitioning: Locate devices behind firewalls capable of deep packet inspection with rulesets limiting access with only approved protocols and functions and to only those devices and endpoints requiring access.
- Anomalous IP traffic: Block and detect anomalous IP traffic and malformed packets. Refer to the Solution section of the CERT-Coordination Center [Vulnerability Note VU#257161](#) for details.
- Disable DHCP on the NMC and configure it to use a static IP address.
- To avoid the use of DNS, set DNS servers to 0.0.0.0 and utilize static IP addresses for all servers the NMC will connect.
- If DNS must be used then normalize DNS through a secure recursive server or application layer firewall
- Enable only secure remote access methods. Disable any insecure protocols.

For devices that must communicate via the Internet:

- Minimize network exposure for embedded and critical devices, keeping exposure to the minimum necessary, and ensuring that devices are not accessible from the Internet unless absolutely essential.
- Ensure communications to devices are via the EcoStruxure IT Gateway. The [EcoStruxure IT platform](#) is security hardened with a mandatory two-factor authentication and high encryption standards. Device data is securely transported to the EcoStruxure IT platform using the EcoStruxure IT Gateway, which uses an outbound connection to minimize risk to your environment.

If network access is not required:

- Remove the Ethernet cable from the SmartSlot NMC, or the embedded NMC Ethernet port if an embedded NMC is present.

Additional mitigations:

- Access Controls: Install physical and logical controls, so that no unauthorized personnel or device can access your systems, components, peripheral equipment, and networks.

Vulnerability Details

Network Management Card Family	Applicable CVE
Network Management Card 1 (NMC1)	CVE-2020-11901 CVE-2020-11909 CVE-2020-11903 CVE-2020-11910 CVE-2020-11904 CVE-2020-11911 CVE-2020-11905 CVE-2020-11912 CVE-2020-11907 CVE-2020-11914 CVE-2020-11908

Network Management Card 2 (NMC2)	CVE-2020-11901 CVE-2020-11902 CVE-2020-11904 CVE-2020-11905 CVE-2020-11906 CVE-2020-11907 CVE-2020-11909 CVE-2020-11910	CVE-2020-11911 CVE-2020-11912 CVE-2020-11913 CVE-2020-11914 CVE-2020-11896 CVE-2020-11898 CVE-2020-11899
Network Management Card 3 (NMC3)	CVE-2020-11901 CVE-2020-11902 CVE-2020-11904 CVE-2020-11905 CVE-2020-11906 CVE-2020-11907 CVE-2020-11909 CVE-2020-11910	CVE-2020-11911 CVE-2020-11912 CVE-2020-11913 CVE-2020-11914 CVE-2020-11896 CVE-2020-11898 CVE-2020-11899

Additional details on these specific vulnerabilities can be found on the ICS-CERT Advisory at <https://www.us-cert.gov/ics/advisories/ICSA-20-168-01>.

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 laptops 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

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, please contact your local Schneider Electric representative and/or Schneider Electric Industrial Cybersecurity Services. These organizations will be fully aware of this situation and can support you through the process.

<https://www.se.com/ww/en/work/support/cybersecurity/overview.jsp>

<https://www.se.com/ww/en/work/services/field-services/industrial-automation/industrial-cybersecurity/industrial-cybersecurity.jsp>

Legal Disclaimer

THIS DOCUMENT IS 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 OF ANY KIND. SCHNEIDER ELECTRIC DISCLAIMS ALL WARRANTIES, EITHER EXPRESS OR IMPLIED, INCLUDING WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. IN NO EVENT SHALL SCHNEIDER ELECTRIC BE LIABLE FOR ANY DAMAGES WHATSOEVER 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. THE USE OF THIS NOTIFICATION, INFORMATION CONTAINED HEREIN, OR MATERIALS LINKED TO IT ARE AT YOUR OWN RISK. SCHNEIDER ELECTRIC RESERVES THE RIGHT TO UPDATE OR CHANGE THIS NOTIFICATION AT ANY TIME AND IN ITS SOLE DISCRETION.

Revision Control:

Version 1 22 June 2020	Original Release
Version 1.1 23 June 2020	Updated Affected Products & Details and Vulnerability Details sections formatting for clarity (pages 2-5)
Version 1.2 5 August 2020	Updated remediation for “Uninterruptible Power Supply (UPS) using NMC2” (page 2)
Version 1.3 6 August 2020	Corrected affected version(s) and enhanced Remediation/Mitigation version details for “Uninterruptible Power Supply (UPS) using NMC2” (page 2)
Version 1.4 1 September 2020	Added remediation for Cooling Products using NMC2 (page 2)
Version 2.0 23 October 2020	Updated overview section, available remediations and affected products tables. New information regarding CVE-2020-11901. Added remediations for “APC 3-Phase Power Distribution Products”, “APC

	<i>Rack Power Distribution Units (PDU)</i> , <i>Rack Automatic Transfer Switches (ATS)</i> , <i>“Environmental Monitoring”</i> (page 1-6)
Version 2.1 <i>18 December 2020</i>	Added remediations for <i>Uninterruptible Power Supply (UPS)</i> using NMC2, <i>APC 3-Phase Power Distribution Products</i> using NMC2, <i>APC Rack Power Distribution Units (PDU)</i> using NMC2, <i>Rack Automatic Transfer Switches (ATS)</i> using NMC2, <i>Environmental Monitoring</i> using NMC2, <i>Cooling Products</i> using NMC2 (page 2-4)
Version 2.2 <i>12 January 2021</i>	Added remediations for <i>Uninterruptible Power Supply (UPS)</i> using NMC3 (page 2)
Version 2.3 <i>30 June 2021</i>	Added remediations for <i>Uninterruptible Power Supply (UPS)</i> , <i>Rack Power Distribution Units (rPDU)</i> , <i>Battery Management</i> , <i>Rack Automatic Transfer Switch (ATS)</i> , <i>Rack Air Removal Unit (RARU)</i> using NMC1, as well as all other remaining NMC1 applications (page 2, 4-6)