

NetShelter™ Rack Power Distribution Units and In-Line Current Meters with NMC3



For APDU9***, and for AP8***, AP7***B, and AP71**B Devices with NMC3

What's in This Document

- Affected Revision Levels 1
- New Features 2
- Fixed Issues 2
- Known Issues 3
- Miscellaneous 3
 - Additional Software and Documentation 3
 - Event Support List 4
 - Hash Signatures 4

Affected Revision Levels

Component	Version	Details
Network Management Card 3 (NMC3) Operating System and NetShelter RPDU Application	AOS: 2.5.5.1 APP: 2.5.3.1	apc_hw21_rpdu2g_2-5-3-1.nmc3
Secure NMC System (SNS) Tool for RPDU	Not applicable	Not applicable
PowerNet® SNMP Management Information Base (MIB)	4.5.8	powernet458.mib

Note: The device's firmware can be upgraded from version 2.5.x.x to 3.x with a subscription to the SNS Tool.

New Features

None.

Fixed Issues

APC Operating System

- Database corruption during power failures or restarts while writing data is now resolved.
- DHCPv6 no longer intermittently reboots when the network interface starts or when the Ethernet cable is reseated.
- You can now send emails as expected if the SMTP server uses an IPv6 address.
- Security fixes:
 - a) The following security vulnerability has been addressed in this release:
CWE-200: Exposure of Sensitive Information to an Unauthorized Actor
SSH Cipher Block Chaining (CBC) cipher has been removed.
 - b) The following third-party components (open source or proprietary) have been updated to address cybersecurity vulnerabilities:
RADIUS Protocol under RFC 2865 - CVE-2024-3596
Implemented support for the Message-Authenticator attribute.
 - c) The following security vulnerabilities have been addressed in this release:
CWE-523: Unprotected Transport of Credentials. Login pages do not use adequate measures to protect the user name and password while they are in transit from the client to the server.
CWE-319: Cleartext Transmission of Sensitive Information. The product transmits sensitive or security-critical data in cleartext in a communication channel that can be sniffed by unauthorized actors.
The user is now referenced as an index rather than their username, for example: NMC/KrtUvuh39YtQmHbyua297g/usercfg.htm?user=2
 - d) The following security vulnerability has been addressed in this release:
CWE-863: Incorrect Authorization
The Network-Only user can only perform actions in the Web UI relevant to the user access level.
 - e) The following security vulnerability has been addressed in this release:
CWE-20: Improper Input Validation
Incoming BACnet packet sizes are now validated.
 - f) The following security vulnerability has been addressed in this release:
CWE-598: Use of GET Request Method With Sensitive Query Strings. This software uses the HTTP GET method to process a request and includes sensitive information in the query string of that request.

Configuration of HSTS is now independent from HTTP or HTTPS configuration. When HSTS is enabled an STS header is added to all responses over HTTPS.

APDU9*, AP8***, AP7***B, and AP71**B Applications**

None

Known Issues

None.

Miscellaneous

Additional Software and Documentation

You can download additional software and documentation from the Schneider Electric download center, www.se.com/ww/en/download.

- 1 Go to www.se.com/ww/en/download.
- 2 Click **Select Location**, then select your location from the provided list. You cannot download software or documentation until you specify your location.
- 3 Use the Search bar and the filter fields to find the needed file.

To find a document, enter the name or part number for your equipment in the Search bar. Then select **Installation & User Guides** under **Document Category**.

To find a firmware file, enter the name or part number for the firmware in the Search bar. Then select **Software & Firmware** under **Document Category**.

Software

The PowerNet MIB allows your SNMP manager to process messages from your RPDU or In-Line Current Meter.

Documentation

- The *MIB Reference Guide* explains the structure of the MIB, types of OIDs, and the procedure to define SNMP trap receivers. You can download the *PowerNet MIB Reference Guide* from www.se.com.
- For information on specific OIDs, use an MIB browser to view their definitions and available values directly from the MIB itself. You can view the definitions of traps at the end of the MIB itself (the file `powernet458.mib`).
- The User Guide for your RPDU or In-Line Current Meter provides comprehensive user instructions, including instructions to recover from a lost password.

Event Support List

To obtain the event names and event codes for all events supported by a currently connected APC by Schneider Electric device, first retrieve the config.ini file from the Network Management Card:

1. Open a connection to the NMC, using its IP Address:
ftp > open <ip_address>
2. Log on using the Administrator user name and password.
3. Retrieve the config.ini file containing the settings of the Network Management Card:
ftp > get config.ini

The file is written to the folder from which you launched FTP.

In the config.ini file, find the section heading [EventActionConfig]. In the list of events under that section heading, substitute 0x for the initial E in the code for any event to obtain the hexadecimal event code shown in the user interface and in the documentation. For example, the hexadecimal code for the code E0033 in the config.ini file (for the event “System: Configuration change”) is 0x0033.

Hash Signatures

apc_hw21_rpdu2g_2-5-3-1.nmc3

MD5 Hash	dfb53f9000e5ccd87a02cd7e382aa25b
SHA-1 Hash	476d65afcf53ba2150e88c845c2d310647195ec1
SHA-256 Hash	19e6471f95a1365111df46ef14b4ab30b68d6a76d1a7183993c84393c69a1630