Version: UPS 15.5
Applicable Models:
==========
ID 1037 with cloud service sku.
SCL: SCL400RMJ1U

This revision provides stronger network data security protection via the below mechanisms to prevent malicious firmware from being upgraded to the UPS through communication interface ports.

Change logs:
1. The mechanism of firmware signing adds to the code in order to protect the UPS from malicious firmware spoofs.

Note: Smart-UPS Firmware Upgrade Wizard tool
always includes the latest released firmware and helps upgrade the UPS code via serial(RS232)port; Upgrade via USB port from this tool is not recommended.
Link to tool - https://www.apc.com/us/en/faqs/FA279197/

Version: UPS 15.1
Applicable Models:
==========
ID 1037 with cloud service sku.
SCL: SCL400RMJ1U

This release includes remediation for the security vulnerabilities listed as CVE-2022-22805, CVE-2022-22806 and CVE-2202-0715 which, if compromised, may allow potential unauthorized access and control of the device.

Change logs:
1. Function implemented to disable UPS firmware upgrades via NMC to mitigate potential risk of malicious UPS firmware being passed through this channel.
2. Enhanced UPS firmware code protection to mitigate the vulnerabilities of unauthorized extraction of confidential firmware and un-authorized network access to SmartConnect UPS.
3. Fix an issue to make the upgrade with Output On feature more stable.

Note: The previous versions may refuse the upgrade with Output On in some special situation. In such cases, please choose a suitable time when the UPS can be turned off without affecting the use of equipment connected to the UPS. Turn off the UPS manually and then upgrade.