Firmware for NPort IA5000 Series (hardware version 2.0 and later) Release Notes

Version: v2.0	Build: 21102111
Release Date: Oct 21, 2021	

Applicable Products

NPort IA5000 Series

Supported Operating Systems

N/A

New Features

• New firmware version for the NPort IA5000 Series V2 models.

Enhancements

N/A

Bugs Fixed

N/A

Changes

N/A

Notes

• The NPort IA5000 Series firmware v2.0 and later versions are incompatible with the older hardware versions of NPort IA5000 Series.
 - Firmware v1.x can only be applied to NPort IA5000 Series hardware version V1.
- Firmware v2.x can only be applied to NPort IA5000 Series hardware version V2 and higher.

Version: v1.7	Build: Build 21032913
Release Date: Mar 31, 2021	

Applicable Products

NPort IA5000 Series

Supported Operating Systems

N/A

New Features

• Supports the MCC Tool.
• Added a notification regarding the limitation on the length of sensitive data.

Enhancements

• Solved security issues: CVE-2017-16715, CVE-2017-14028, CVE-2017-16719, CVE-1999-0511.

Bugs Fixed

• NPort might hang when using in a public network.
• NPort did not send SNMP Authentication Failure trap.
• Unable to get complete network info when max connection was full with NPort Fixed TTY driver.
• Force transmit time could work when it was set at 20 ms in UDP operation mode.
• The default gateway was invalid when the IP address ended with ".0".
• NPort sent a DUP ACK while handshaking.
• Saved configuration from the DHCP server to flash too frequently.

Changes

N/A

Notes

• This version of the firmware can be applied only to hardware version 1.x. Download firmware v2.x for NPort IA5000 Series hardware version V2 and higher.

Version: v1.6	Build: Build 17060616
Release Date: Jul 04, 2017	

Applicable Products

NPort IA5000 Series

Supported Operating Systems

N/A

New Features

N/A

Enhancements

• Enhanced web login security and supports 5 users logged in simultaneously.
• Extended HTTP challenge ID length from 32 bits to 256 bits.
• Enabled the default password "moxa".
• Increased CSRF protection mechanism.
• Increased XSS protection mechanism.

Bugs Fixed

• The user's password and SNMP community name may be exposed by a buffer overflow issue.
• NPort may reboot or hang from several buffer overflow attacks through Telnet, SSH, DSCI, SNMP, HTTP, and HTTPS.
• TCP/IP protocol may stop responding: CNCERT CNVD-2016-12094.
• In pair connection mode, master will not pull down RTS/DTR signal after the TCP connection is broken.

Changes

N/A

Notes

N/A