Firmware for NPort 5600 Series Release Notes

Version: v3.12	Build: 24092017
Release Date: Nov 20, 2024	

Applicable Products

NPort 5600 Series

Supported Operating Systems

N/A

New Features

N/A

Enhancements

- Upgrades mbedTLS to v2.28.8.
- Disables SNMP by default.

Bugs Fixed

- Account set via NPort Administrator-Configuration may fail.
- Using the event group OpMode in the remote log may cause the NPort to reboot.
- MXview One can't recognize NPort 5000 Series with SNMPv3.
- NPort may send abnormal DHCP request when using DHCP relay.
- NPort may append unnecessary options to the DHCP request.
- Security issue: HTML XSS attack prevention on certain web pages.
- Correct the data packing feature when the delimiter buffer is full.
- A potential problem of a variable going out of bound.
- IP filtering Plus setting not included when exporting the configuration file.
- An invalid fd input in FD_ISSET API causing unexpected behavior and DUT crash.

Changes

N/A

Notes

- For firmware version prior to v3.10, first upgrade to the intermediate firmware version v3.11 before upgrading to this version.

Version: v3.11	Build: 21061519
Release Date: Jun 16, 2021	

Applicable Products

NPort 5600 Series

Supported Operating Systems

N/A

New Features

N/A

Enhancements

• Supports HW Rev. 2.0 and prior revisions of NPort 5610 and NPort 5630 models.

Bugs Fixed

• Firmware v3.10 does not support HW Rev. 2.0 and prior revisions of NPort 5610 and NPort 5630 models.
• Firmware upgrade through the web console is prohibited.

Changes

N/A

Notes

• This is the intermediate firmware version for upgrading to firmware v3.1x and later

Version: v3.10	Build: Build 21032913
Release Date: Mar 31, 2021	

Applicable Products

NPort 5600 Series

Supported Operating Systems

N/A

New Features

- Supports remote log function.
- Supports turning on HTTPS with TLS 1.2 by default.
- Supports MXconfig v2.6 and MXview v3.1.20.
- Added a notification regarding the limitation on the length of sensitive data.

Enhancements

- Solved security issues: CWE-319, CVE-2020-1938, CVE-2013-0631.
- Records username, source IP, and port number in "Event Log" and "System Log".
- Upgraded mbedTLS to v2.7.15.
- Disables Telnet console by default.
- Disables TLS 1.0/1.1 by default.
- Adds an account lockout mechanism for web, Telnet, and MOXA service.
- Removes SSL 2.0 and lower (keep TLS 1.0/1.1/1.2).
- Improved the UI and UX on "Configuration file import/export and pre-shared key".
- Extended the validity period of the certificate.
- Rejects an unrecognized host header when HTTP is configurable.

Bugs Fixed

- NPort sent a DUP ACK while handshaking.
- TNPort would still send "ALIVE" command packets after serial data had been transmitted.
- Saved configuration from the DHCP server to flash too frequently.
- An email event could not be sent while the SNMP service was disabled.
- The default gateway was invalid when the IP address ended with ".0".
- The connection status could not be displayed correctly in NPort Administrator—Port Monitor.
- TCP client mode could not connect to TCP server mode on the same NPort.
- Account's password could not be set correctly via NPort Administration Suite 1.x version.
- The device might restart after getting the SNMP MIB value of tcpConnRemPort.
- The NPort might send a duplicate ACK in TCP server mode while doing a handshake.
- The operation mode RFC2217 was missing.
- Sent NTP requests frequently when NTP connection failed.
- Syslog server could not receive Cold Start event log when DUT's IP was assigned by the DHCP server.
- The message of NTP sync success was not easy to clarify.
- The message of the logout page showed the incorrect device model name.
- NPort would respond to system time for "timestamp" ICMP packet.
- Web server would respond to nonexistent file.

Changes

N/A

Notes

- Applicable to NPort 5610/5630 hardware revision 3.0 and later.
- Applicable to all NPort 5650 hardware revision.

Version: v3.9	Build: Build 19032122
Release Date: Mar 29, 2019	

Applicable Products

NPort 5600 Series

Supported Operating Systems

N/A

New Features

• Supports HTTPS.
• Supports MXview auto-topology function.
• Supports MXconfig.
• Supports SNMPv2c.
• Supports IGMP.

Enhancements

• Accessible IP list can now be used to restrict all device services.
• Complies with Moxa Security Guidelines on the following: Account Authentication Management, Network Service Management, and Audit and Log Management.
• CVE-2017-14028: An attacker may be able to exhaust memory resources by sending a large amount of TCP SYN packets.
• CVE-2017-16715: An attacker may be able to exploit a flaw in the handling of Ethernet frame padding that may allow for information exposure.
• CVE-2017-16719: An attacker may be able to inject packets that could potentially disrupt the availability of the device.
• Updates the web UI.

Bugs Fixed

• NPort does not send SNMP Authentication Failure trap.
• Pair connection mode cannot resolve the domain name.
• Unable to get complete network info when the max connection is full with the NPort Fixed TTY driver.
• The password may be exposed in the MOXA service.

Changes

N/A

Notes

N/A

Version: v3.8	Build: Build 17030709
Release Date: Mar 14, 2017	

Applicable Products

NPort 5610-8, NPort 5610-8-48V, NPort 5630-8, NPort 5610-16, NPort 5610-16-48V, NPort 5630-16, NPort 5650-8, NPort 5650-8-M-SC, NPort 5650-8-S-SC, NPort 5650-8-T, NPort 5650-8-HV-T, NPort 5650-16, NPort 5650-16-M-SC, NPort 5650-16-S-SC, NPort 5650-16-T, NPort 5650-16-HV-T

Supported Operating Systems

N/A

New Features

N/A

Enhancements

N/A

Bugs Fixed

• The user's password and SNMP community name may be exposed by a buffer overflow issue.

Changes

N/A

Notes

N/A

Version: v3.7	Build: Build 16082411
Release Date: N/A	

Applicable Products

NPort 5610-8, NPort 5610-8-48V, NPort 5630-8, NPort 5610-16, NPort 5610-16-48V, NPort 5630-16, NPort 5650-8, NPort 5650-8-M-SC, NPort 5650-8-S-SC, NPort 5650-8-T, NPort 5650-8-HV-T, NPort 5650-16, NPort 5650-16-M-SC, NPort 5650-16-S-SC, NPort 5650-16-T, NPort 5650-16-HV-T

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.
• The IP address of the NPort can be set to an address ending with 0 or 255.

Bugs Fixed

• NPort cannot send e-mail using Google's SMTP server.
• In pair connection mode, master does not pull down RTS/DTR signal after the TCP connection is broken.
• Command port sends lots of "D_ASPP_CMD_ALIVE" packets after running for 50 days.
• NPort may reboot or hang from several buffer overflow attacks through Telnet, SSH, DSCI, SNMP, HTTP, and HTTPS.

Changes

N/A

Notes

N/A

Version: v3.6	Build: Build 15041515
Release Date: N/A	

Applicable Products

NPort 5610-8, NPort 5610-8-48V, NPort 5630-8, NPort 5610-16, NPort 5610-16-48V, NPort 5630-16, NPort 5650-8, NPort 5650-8-M-SC, NPort 5650-8-S-SC, NPort 5650-8-T, NPort 5650-8-HV-T, NPort 5650-16, NPort 5650-16-M-SC, NPort 5650-16-S-SC, NPort 5650-16-T, NPort 5650-16-HV-T

Supported Operating Systems

N/A

New Features

N/A

Enhancements

• Uses model name instead of "NULL" for SNMP object "sysDescr".
• Supports connecting to the server by domain name and the server IP will change dynamically.
• Supports updating the ARP table by gratuitous ARP.
• Supports time synchronization with an NTPv4 server.
• Supports RFC2217 NOTIFY-LINESTATE for Transfer Shift Register Empty and Transfer Holding Register Empty.

Bugs Fixed

• If an SNMP GETNEXT command is issued on an object that does not exist, 'no such name error' is displayed.
• When DHCP renews IPs, if the IP was originally given by a relay agent, NPort should send a DHCP request to the relay agent, not the DHCP server.
• In Real COM mode, when the modem status of the NPort's serial port is changed frequently, the NPort will sometimes fail to notify the change to the driver.
• In reverse telnet mode, the NPort will try to subnegotiate the COM port control options without option negotiation first.
• In RFC2217 Mode, if the Ethernet data has many FF characters, some data may be lost while passing the data to the serial side.

Changes

N/A

Notes

N/A