Firmware for NPort 5200A Series Release Notes

Version: v1.6	Build: Build 20101317
Release Date: Oct 15, 2020	

Applicable Products

N/A

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 v3.2.
• A notification regarding the limitation on the length of sensitive data.

Enhancements

• Solved Nessus CVSS v3.0 issues, which scores exceeded 7 and above.
• Solved security issues.
• 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.
• Added an account lockout mechanism for web, Telnet, and MOXA service.
8: Removed SSL 2.0 and lower (keep TLS 1.0/1.1/1.2).
• Improved UI and UX on "Configuration file import/export and pre-shared key".

Bugs Fixed

• TCP used to duplicate ACK while handshaking.
• The NPort would still send "ALIVE" command packets after serial data has been transmitted.
• Configuration from DHCP server will be saved to flash frequently.
• An email event could not be sent while the SNMP service was disabled.
• The system became invalid when the IP address ended with ".0"
• 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 system would cold start after receiving MIB tcp Connection Remote Port (tcpConnRemPort).

Changes

N/A

Notes

N/A

Version: v1.5	Build: Build 19032122
Release Date: Mar 29, 2019	

Applicable Products

NPort 5200A Series

Supported Operating Systems

N/A

New Features

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

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.
• Remove unnecessary information displayed on the Web, Telnet, and Serial consoles during the login process.
• Remove the TTL limitation (1) on multicast packets.

Bugs Fixed

• Pair connection mode cannot resolve the domain name.

Changes

N/A

Notes

N/A

Version: v1.4	Build: Build 17030709
Release Date: Mar 15, 2017	

Applicable Products

NPort 5210A, NPor 5230A, NPort 5250A, NPort 5210A-T, NPort 5230A-T, NPort 5250A-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 buffer overflow issue.

Changes

N/A

Notes

N/A

Version: v1.3	Build: Build 1610041
Release Date: N/A	

Applicable Products

NPort 5210A, NPor 5230A, NPort 5250A, NPort 5210A-T, NPort 5230A-T, NPort 5250A-T

Supported Operating Systems

N/A

New Features

N/A

Enhancements

• Enhance web login security and support 5 users login simultaneously.
• Extend HTTP's challenge ID length from 32 bits to 256 bits.
• Enable default password as "moxa".
• Increase CSRF protection mechanism.
• Increase XSS protection mechanism.
• IP of NPort Can be set to address ending with 0 or 255.
• Support "ARP probe" in RFC5227. NPort would response for ARP requests with sender IP address 0.0.0.0.

Bugs Fixed

• NPort can't send e-mail by using Google's SMTP server.
• In pair connection mode, master doesn't pull down RTS/DTR signal after TCP connection is broken.
• Command port sends lots of "D_ASPP_CMD_ALIVE" packets after running 50 days.
• Connect too many connection to HTTP server at the same time will block the new connection for a while.
• NPort may reboot or hang under serveral buffer overflow attacks on Telnet, SSH, DSCI, SNMP,

Changes

N/A

Notes

N/A

Version: v1.2	Build: Build 15041515
Release Date: N/A	

Applicable Products

NPort 5210A, NPor 5230A, NPort 5250A, NPort 5210A-T, NPort 5230A-T, NPort 5250A-T

Supported Operating Systems

N/A

New Features

N/A

Enhancements

• Use model name instead of "NULL" for SNMP object "sysDescr".
• Support connecting to the server by domain name and server's IP would change dynamically.
• Support updating ARP table by gratuitous ARP.
• Support RFC2217 NOTIFY-LINESTATE for Transfer Shift Register Empty and Transfer Holding Register Empty.

Bugs Fixed

• If a GETNEXT command of SNMP is issued on an object that does not exist, it displays 'no such name error'.
• In DHCP renewing IP stage, if the IP was originally given by a relay agent, NPort should send DHCP Request to relay agent, not the DHCP server.
• In Real COM mode, when modem status of the NPort's serial port is changed frequently, NPort sometimes fail to notify the change to the driver.
• NPort under reverse telnet mode try to sub-negotiate the COM port control options without option negotiation first.
• In RFC2217 Mode, when the data from ethernet side have many FF characters, some data may be lost on serial side.
• Modified parsing data mechanism to fix import file fail.
• Customer is unable to see the baud rate by using Telnet console at "Veiw settings".

Changes

N/A

Notes

N/A