Firmware for NPort IA5000A Series (NPort IA5150A models) Release Notes

Version: v1.6	Build: 24092017
Release Date: Nov 20, 2024	

Applicable Products

NPort IA5250AI-T, NPort IA5150A, NPort IA5150A-T, NPort IA5150AI, NPort IA5150AI-T, NPort IA5250A, NPort IA5250A-T, NPort IA5250AI

Supported Operating Systems

N/A

New Features

N/A

Enhancements

- Adds a configuration setting to reject an unrecognized host header in HTTP.
- Upgrades mbedTLS to v2.28.8.
- Disables SNMP by default.

Bugs Fixed

- Web console cannot be accessed via dual IP.
- 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.
- Incorrect data packing 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

N/A

Version: v1.5	Build: Build 21022213
Release Date: Mar 02, 2021	

Applicable Products

NPort IA5150A/IA5250A 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 v3.2.
- 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.
- 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".
- Extended the validity period of the certificate.

Bugs Fixed

- TCP used to duplicate ACK while handshaking.
- The NPort would still send "ALIVE" command packets after serial data has been transmitted.
- The configuration from the DHCP server would 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"
- 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.
- Send NTP requests frequently when NTP connected failed.
- Syslog server cannot receive Cold Start event log when DUT's IP is assigned by DHCP server.
- The message of NTP sync success is not easy to clarify.
- The message on the logout page shows an incorrect device model name.

Changes

N/A

Notes

N/A

Version: v1.4	Build: Build 19032122
Release Date: Mar 29, 2019	

Applicable Products

NPort IA5150A/IA5250A Series

Supported Operating Systems

N/A

New Features

• Supports HTTPS.
• Supports MXview auto-topology function.
• Supports MXconfig.
• Supports SNMPv2c.
• Supports dual IP.
• Supports redundant LAN.

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: v1.3	Build: Build 16100514
Release Date: Nov 10, 2016	

Applicable Products

NPort IA5150A, NPort IA5150AI, NPort IA5150AI-T, NPort IA5150A-T, NPort IA5250A, NPort IA5250AI, NPort IA5250AI-T, NPort IA5250A-T, NPort IA5150A-IEX, NPort IA5150AI-IEX, NPort IA5150AI-T-IEX, NPort IA5150A-T-IEX, NPort IA5250A-IEX, NPort IA5250AI-IEX, NPort IA5250AI-T-IEX, NPort IA5250A-T-IEX

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.
• Supports "ARP probe" in RFC5227. NPort would respond for ARP requests with sender IP address 0.0.0.0.

Bugs Fixed

• NPort cannot send email 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: v1.2	Build: Build 15041515
Release Date: N/A	

Applicable Products

NPort IA5150A, NPort IA5150AI, NPort IA5150AI-T, NPort IA5150A-T, NPort IA5250A, NPort IA5250AI, NPort IA5250AI-T, NPort IA5250A-T, NPort IA5150A-IEX, NPort IA5150AI-IEX, NPort IA5150AI-T-IEX, NPort IA5150A-T-IEX, NPort IA5250A-IEX, NPort IA5250AI-IEX, NPort IA5250AI-T-IEX, NPort IA5250A-T-IEX

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.
• Modified parsing data mechanism to fix import file failure.
• Unable to see the baud rate through a Telnet console on the "View settings" side.
• System reboots when receiving IGMP packets.
• The trap settings for port auto warning in the configuration file will be set to email settings after import.
• When both serial ports are set to TCP server mode, the connection on port 1 works normally, but will fail after a connection on port 2 is established.

Changes

N/A

Notes

N/A