



## Firmware for NPort W2150A/W2250A Series Release Notes

<b>Version: v2.3</b>	<b>Build: Build 21100808</b>
<b>Release Date: Apr 22, 2022</b>	

### Applicable Products

NPort W2150A/W2250A Series

### Supported Operating Systems

N/A

### New Features

- Supports a second source for RJ45 PHY and RTC (real-time clock).

### Enhancements

- Improves compatibility with Huawei access points when Ethernet bridge mode is enabled.
- Improves the performance of wireless connections in high-noise environments.
- The Linux kernel hardcoded MSS value 48 bytes is now optimized based on actual requirements to prevent vulnerabilities and wastage of resources.
- The device will not be allowed to roam between APs when fast roaming is disabled.

### Bugs Fixed

- NTP request is not sent every 10 minutes as per the requirement.
- System freezes when the serial parameters are changed frequently.
- Incorrect RF type value on the WLAN Status page.
- The NPort W2x50A incorrectly connected to an access point that was not supported by its RF type.
- The NPort W2x50A has trouble finding an available access point when fast roaming is enabled.
- In UDP mode, NPort cannot broadcast to its peers if the starting IP is a broadcast IP with Ethernet bridge mode enabled.
- CVE-2019-11477: An integer overflow occurred in the kernel when handling TCP Selective Acknowledgments (SACKs).
- CVE-2019-11478: The TCP retransmission queue implementation in tcp\_fragment of the kernel gets fragmented when handling certain TCP Selective Acknowledgment (SACK) sequences.
- CVE-2019-11479: The Linux kernel default MSS was hardcoded to 48 bytes.
- The local listening port cannot be modified in the UDP mode.
- Changed Host Name to Sever Name in the DHCP Option 12 request.

### Changes

N/A

### Notes

- Firmware upgrade path: If you are upgrading from a version prior to firmware v1.11, you must first upgrade to v1.11 before upgrading to v2.x or later. This upgrade path is for enhancing the system security. Please contact the Moxa TS team for firmware v1.11 or if you need help with your firmware upgrade.



<b>Version: v2.2</b>	<b>Build: Build 18082311</b>
<b>Release Date: Jan 15, 2019</b>	

### **Applicable Products**

NPort W2150A, NPort W2150A-T, NPort W2250A, NPort W2250A-T

### **Supported Operating Systems**

N/A

### **New Features**

N/A

### **Enhancements**

- Improved the fast roaming algorithm.
- In Real COM and TCP server mode, connection will be reset when the connection number has already reached the "max connection number".
- Reduced TCP retransmission timeout based on "TCP alive check time".
- Prevents wireless connections from reconnecting frequently.
- Prevents XSS attacks on webpage.
- Prevents CSRF attacks on webpage.
- Prevents potential command injection on webpage.
- Enhanced client authentication on web login page.
- Removed the wording below the goahead logo.

### **Bugs Fixed**

- When fast roaming is enabled, NPort may roam to a non-selected channel.
- Goahead vulnerability(CVE-2017-17562), which caused the webpage to crash.
- Buffer overflow issue on TCP port 4900.

### **Changes**

N/A

### **Notes**

N/A



<b>Version: v2.1</b>	<b>Build: Build 17112017</b>
<b>Release Date: N/A</b>	

### **Applicable Products**

NPort W2150A, NPort W2150A-T, NPort W2250A, NPort W2250A-T

### **Supported Operating Systems**

N/A

### **New Features**

N/A

### **Enhancements**

N/A

### **Bugs Fixed**

- WPA2 KRACK vulnerabilities which are associated with the following CVE identifiers: CVE-2017-13077, CVE-2017-13078, CVE-2017-13079, CVE-2017-13080, CVE-2017-13081, CVE-2017-13082, CVE-2017-13084, CVE-2017-13086, CVE-2017-13087, and CVE-2017-13088.
- W2x50A can connect to some APs that are using 802.11n, but cannot launch a web or telnet console.

### **Changes**

N/A

### **Notes**

N/A



<b>Version: v2.0</b>	<b>Build: Build 17081115</b>
<b>Release Date: N/A</b>	

**Applicable Products**

NPort W2150A, NPort W2150A-T, NPort W2250A, NPort W2250A-T

**Supported Operating Systems**

N/A

**New Features**

- Modified firmware structure for security purposes; please upgrade to v1.11 before upgrading to v2.0.

**Enhancements**

- Supports new architecture of NPort W2x50A firmware.

**Bugs Fixed**

N/A

**Changes**

N/A

**Notes**

N/A



<b>Version: v1.11</b>	<b>Build: Build 17081115</b>
<b>Release Date: N/A</b>	

### **Applicable Products**

NPort W2150A, NPort W2150A-T, NPort W2250A, NPort W2250A-T

### **Supported Operating Systems**

N/A

### **New Features**

N/A

### **Enhancements**

- Supports accepting encrypted firmware for v2.0 and above.
- Added a default password.
- Improved the wireless stability when signal strength is low.
- Upgraded openssl to openssl-1.0.2k.
- Upgraded dropbear SSH to dropbear-2016.74.

### **Bugs Fixed**

- When fast roaming is enabled and the wireless signal is better than the roaming threshold for a long time, sometimes data may not be able to be sent out.
- WLAN could not pass RADIUS authentication when security is set to EAP-TLS.
- When bridge mode is enabled, NPort may not function properly after receiving PROFINET packets.

### **Changes**

N/A

### **Notes**

N/A



<b>Version: v1.10</b>	<b>Build: Build 16113018</b>
<b>Release Date: N/A</b>	

### **Applicable Products**

NPort W2150A, NPort W2150A-T, NPort W2250A, NPort W2250A-T

### **Supported Operating Systems**

N/A

### **New Features**

N/A

### **Enhancements**

- Supports 802.11n in Infrastructure mode.
- Supports W2X50A-CN.
- Supports WLAN log.
- Supports new site survey on general profile setting page.
- Shows RSSI and current BSSID on WLAN status page.
- Upgraded glibc to v2.18.
- Modified the fast roaming mechanism, which is triggered by low signal (RSSI).
- Removed password related items from snmp.
- Supports import/export by DSU.

### **Bugs Fixed**

- The "Connection goes down" function may not work correctly in Real COM mode for W2250A Port 2.
- Sometimes the device may not be able to establish a wireless connection after booting up.
- W2x50A may not be able to connect to any APs for a long time, and sometimes it cannot recover.
- When fast roaming is enabled and the wireless signal is unstable for a long time, sometimes data may not be able to be sent out.
- When Ethernet bridge is enabled, sometimes data may not be able to be sent out.
- When Ethernet bridge is enabled, IP conflict checks may not work on the WLAN side.
- Ready LED may not blink red when IP conflicts are detected.
- The local time may not be correct when changing the time zone setting.
- GHOST vulnerability: ICS-CERT CVE-2015-0235.
- DROWN attack issue: ICS-CERT CVE-2016-0800.

### **Changes**

N/A

### **Notes**

N/A