Firmware for TN-5900 Series Release Notes

Version: v3.4	Build: 23051916
Release Date: Jun 15, 2023	

Applicable Products

TN-5900 Series

Supported Operating Systems

N/A

New Features

N/A

Enhancements

N/A

Bugs Fixed

Vulnerability [MPSA-230401]
Vulnerability [MPSA-230402]

Changes

N/A

Notes

N/A

Version: v3.3	Build: 22101415
Release Date: Nov 01, 2022	

Applicable Products

TN-5916-WV-CT-T, TN-5916-WV-T

Supported Operating Systems

N/A

New Features

NA

Enhancements

• Improved the certificate management code quality.

Bugs Fixed

• [Web] Users are able to modify the Certificate Authority (CA) name of the device's URL.
• [Certificate Management] The system does not properly check for special characters in the Certificate Management section of the web UI.
• [System] The system does not properly check for special characters for configuration parameters.
• [Vulnerability] MPSA-221103
• [Vulnerability] MPSA-221104

Changes

NA

Notes

N/A

Version: v3.2	Build: N/A
Release Date: Sep 20, 2022	

Applicable Products

TN-5900 series

Supported Operating Systems

N/A

New Features

• Added support for firewall logs including L3 policy, DoS, and Trusted Access events.
• Users can now create and edit NAT rules through SNMP.
• Added a percentage representation for CPU and Memory Usage.
• Added support for Ethernet port bandwidth limitation.
• Added support for DHCP Relay Agent.
• Added support for configuration version control.
• Added support for the Zone bridge interface.

Enhancements

• [NAT] Added the interface to the NAT settings in the MIB file.
• [Bridge] Increased the maximum number of Bridge interfaces to 8.

Bugs Fixed

• [Port Setting] Flow Control cannot be enabled on Ethernet ports.
• [Port Setting] When checking the Ethernet port status using the CLI, the port's Flow Control status shows incorrectly.
• [Static Route] Users are able to create multiple static unicast routes with identical names.
• [Static Route] Users are unable to create a default static unicast route rule with value 0.0.0.0.
• [Web] The web interface does not check if the user-specified IGMP query interval range is valid. This issue does not affect the CLI.
• [Web] The configuration file shows incorrect WAN interface information.
• [Web] The "Policy Setup" page displays differently in different web browsers.
• [Web] The password and key are displayed in plain text in the web interface.
• [Web] The NAT configuration page displays incorrectly when using the Internet Explorer browser.
• [Web] Users are unable to modify static unicast routing rules in the web interface.
• [Firewall] After configuring policies in the firewall configuration section, the configuration takes several minutes before taking effect.
• [ABC-01] The system does not record an event log when encountering issues while importing from or exporting to the ABC-01.
• [ABC-01] When importing from or exporting to the ABC-01 when no connection is established, the Fault LED does not light up.
• [ABC-01] Users will be randomly logged out from the web interface when the ABC-01 has finished importing or exporting the configuration.
• [NAT] Users are unable to configure port forwarding using MIB files.
• [NAT] Exporting the configuration will fail if a NAT interface is removed.
• [CLI] The password and key are displayed in plain text in the CLI.
• [System] If MD5 is selected as the Authentication Type for the OSPF interface, importing the configuration will fail.
• [System] The device hangs during startup, preventing users from accessing the device using any interface.
• [Event Log] The system does not record an event log when the DHCP server configuration is changed.
• [Bridge] The Bridge interface configuration is incorrect during system startup.

• [Vulnerability] LLDP memory leak.
• [Vulnerability] SNMP CVE-2020-15862, CVE-2020-15861, CVE-2018-18066, CVE-2018-18065, CVE-2014-2284, CVE-2012-6151, CVE-2012-2141.
• [Vulnerability] OpenSSL CVE-2019-1563, CVE-2019-1559, CVE-2019-1552, CVE-2019-1547, CVE-2018-5407, CVE-2018-0739, CVE-2018-0737, CVE-2018-0734, CVE-2018-0732, CVE-2017-3738, CVE-2017-3737, VE-2017-3736, CVE-2016-8610, CVE-2016-7055, CVE-2016-6303, CVE-2016-6302, CVE-2016-2182, CVE-2016-2181, CVE-2016-2180, CVE-2016-2179, CVE-2016-2178, CVE-2016-2177, CVE-2016-2176, CVE-2016-2109, CVE-2016-2107, CVE-2016-2106, CVE-2016-2105.
• [Vulnerability] Linux CVE-2019-15666.
• [Vulnerability] Vulnerability issue: W-2020-0121.
• [SMC Route] Abnormal interaction behavior between VRRP and Static Multicast Route (SMC).
• [SMC Route] Potential multicast routing looping issue.
• [OSPF] If the OSPF Auth Key is set to 8 digits, importing configurations will fail.
• [Event Log] After rebooting the device, the severity of the Link up/down event log is recorded incorrectly.
• [Trusted Access] When importing a configuration file, Trusted Access settings are not updated correctly.
• [DHCP] If the hex option is configured for DHCP Server Option82, it may cause the DHCP server to crash.
• [DHCP] Long RID/CID values in the DHCP server settings may cause word string overlapping in the web interface.
• [DHCP] Users can configure an overlapping IP range for the DHCP server in the web interface.

Changes

• [NAT] Added compatibility for legacy configurations.
• [DDoS] Changed the ARP Flood limit parameter in DoS settings to only count ARP requests.
• [Bridge] Added a Bridge Interface configuration page to the web interface.
• [Bridge] Added the bridge interface name prefix to every bridge member in the L2/L3 firewall interface.
• [DHCP] Adjusted the DHCP Option 82 CID/RID input size to be the same as the DHCP Relay Agent.

Notes

N/A

Version: v3.1	Build: TN5916_V3.1_Build_20040717
Release Date: Jul 22, 2020	

Applicable Products

TN-5900 Series

Supported Operating Systems

N/A

New Features

• Added support for L3 firewall rules on the bridge interface.
• Added support for VRRP NAT Binding.

Enhancements

N/A

Bugs Fixed

• The IGMP web UI shows the wrong querier port when the TRv2 port is set as the querier port.
• IGMP Snooping forwards packages back to the source port in TRv2.
• The DHCP server would sometimes not work properly after a power cycle.
• IGMP causes heavy CPU load due to multicast traffic flood on the bridge port.
• An unexpected value is added when exporting the firewall configuration.
• UDP communication with the bridge port would sometimes drop when using TRv2.
• The Multicast Forwarding Table web UI page shows abnormal values.

Changes

N/A

Notes

N/A

Version: v3.0	Build: N/A
Release Date: Dec 16, 2019	

Applicable Products

N/A

Supported Operating Systems

N/A

New Features

- Support Security Guideline Level 2, including Auto-logout, Default Password, Encrypted Account Password, Password Policy, Radius for Web Login, Encrypted Configuration File Export, and Key/Certificate of SSL/SSH Management
- Support NAT, including Bi-direction 1-1 NAT, Bi-direction N-1 NAT, Bi-direction Port Forwarding NAT, and 512 NAT rules
- Support L2 Firewall, L3 Firewall, and Bridge Mode
- Support DHCP Server with Option 66/67/82
- Support DHCP Client with Option 66/67
- Support PIM-SM
- Support DVMRP
- Support OSPF
- Support VRRP
- Support DNS Server
- Support IPSec, L2TP
- Support IEEE802.1x
- Support MXstudio

Enhancements

- Support SNMPv3 AES/DES Encryption Type
- Support Port Status and Interface Status on Web UI
- Upgrate NTP Server to ntp-4.2.8p13
- Set Trunk Port to Auto-negotiation by Default
- Use Javascript for Statistics Monitoring on Web UI
- Support CLI-based Configuration Export
- Support 12-digit Serial Number
- Support HTTPS Certificate using SHA256 with 2048 Key Length
- Upgrade OpenSSH to v7.5p1

Bugs Fixed

- Fix bug that Static Route doesn't work after importing configuration
- Fix CLI Command Injection issue
- Fix bug that MAC aging time doesn't work after importing configuration or port linking down and up
- Fix bug that Turbo Ring V2 sends lots of topology changes after rebooting
- Fix but that NTP date doesn't synchronize with RTC immediately
- Fix bug that CLI command "clock set <hh:mm:ss>" doesn't work
- Fix bug that Port still links up after Trunk Port is disabled
- Fix bug that physical port is not configured correctly when Trunk Port setting is involved
- Fix bug that Relay Bypass causes interface down and up instantly

Changes

N/A

Notes

N/A

Version: v1.2	Build: N/A
Release Date: Dec 16, 2015	

Applicable Products

N/A

Supported Operating Systems

N/A

New Features

N/A

Enhancements

N/A

Bugs Fixed

N/A

Changes

N/A

Notes

N/A