Firmware for PT-G503 Series Release Notes

Version: v5.3	Build: N/A
Release Date: Sep 28, 2023	

Applicable Products

PT-G503 Series

Supported Operating Systems

N/A

New Features

• Support New MOXA commands:
  - change network setting
  - broadcast search
  - import config (sys,ini)
  - import cli
  - upgrade firmware (firmware.rom)
  - export plaintext config
  - export encrypted config
  - get device information
  - verify account
  - add/remove account
  - register a web session id
  - set mac address
 - export debug log
 - factory default
 - load commands from a file and sent to the DUT
 - Perform broadcast search 100000 times

Enhancements

• Upgrades JavaScript library to jquery-3.7.0.min.js.
• Upgrades SSH package (dropbear_2019.78) to support “hmac-sha2-256 & diffie-hellman-group14-sha256”.

Bugs Fixed

• [CVE-2021-27417] If the file size is exceptionally large, undefined behavior can’t be prevented.
• [CVE-2022-40691] A specially crafted HTTP request can lead to disclosure of sensitive information.
• [CVE-2022-40214] Potential tampered messages.
• [MSRV-2019-003] Denial of Service (web service) by improper HTTP GET command (CNVD-2019-116145).
• [MSRV-2019-004] Denial of Service (web service) by over-sized (more than 12 MB) firmware upgrade through HTTP/HTTPS.
• [MSRV-2019-005] Denial of Service (web service) by excessive length of HTTP GET command.
• [MSRV-2017-011] Cross-Site Request Forgery (CSRF) vulnerability
• [MSRV-2017-021] Release the cookie once the session expires to avoid the old cookie value being reused.
• [CVE-2022-0778] Import certificate issue: Updates OpenSSL package.
• [TALOS-2022-1619] A specially crafted HTTP request can lead to an arbitrary JavaScript execution,
• [TALOS-2022-1618] A specially crafted HTTP message header can lead to denial of service.
• [TALOS-2022-1616] A specially crafted network sniffing can lead to the disclosure of sensitive information.

• [TALOS-2022-1621] A specially crafted HTTP request can lead to the disclosure of sensitive information.
• [nessus-43156] The remote network time service has a denial-of-service vulnerability.
• [nessus-97861] The remote NTP server responds to mode 6 queries, which can potentially be used in NTP amplification attacks.
• [Nessus-85582]: Web application potentially vulnerable to clickjacking
• XSS vulnerability on the following pages:
  - LLDP diagnostic page
  - Time page (1st Time Server IP/Name & 2nd Time Server IP/Name)
  - Remote TFTP page (all input fields)
  - SNMP Settings page (Admin/User Data Encryption Key, 1st Trap Server IP/Name, 2nd Trap Server IP/Name)
  - Email Setup page (email address)
  - DHCP Relay Agent page (Value)
• PTP port stuck in listening state. PTP port should change its role from slave to master so that the device under it can sync with it to update the time.
• After NTP local time is set, if there are two NTP servers, NTP function does not work properly resulting in time sync failure.
• The username and password configured on the SNMP settings page can be viewed in plaintext using browser-based tools.

Changes

• HTTP and SNMP is disabled by default on the Management interface.
• Modifies relay behavior: power on relay to NO, power off relay to NC
• VRRP advertisement packet will be forwarded to I port from A/B port.
• Removes the wording "IE 11" on the web browser.
• Removes weak ciphers CBC and SHA1 from TLSv1.2.
• Replaces Monitoring page with a non-Java version.

Notes

• We recommend upgrading the firmware from version 5.2 to version 5.3 through HTTP, TFTP, and XMODEM. Please note that using HTTPS for the upgrade is not recommended.

Version: v5.2	Build: N/A
Release Date: Aug 02, 2022	

Applicable Products

N/A

Supported Operating Systems

N/A

New Features

- Added the Nodes Table, which displays supervision frame information.
- Added support for RSTP Grouping in HSR mode.
- Users can now customize the IED name in the MMS feature.

Enhancements

- Added for support for TLS 1.2.

Bugs Fixed

N/A

Changes

N/A

Notes

N/A

Version: v5.1	Build: N/A
Release Date: Apr 13, 2022	

Applicable Products

N/A

Supported Operating Systems

N/A

New Features

N/A

Enhancements

N/A

Bugs Fixed

- The PTP boundary clock Best Master Clock algorithm behaves abnormally.
- The P2P path delay correction field does not update correctly.
- The SNMP polling function for MXview always fails.
- Forcing the port speed to 100M/10M in the Web UI does not work.

Changes

N/A

Notes

N/A

Version: v5.0	Build: Build_18071716
Release Date: Dec 09, 2019	

Applicable Products

PT-G503 Series

Supported Operating Systems

N/A

New Features

• The flash memory had been replaced.

Enhancements

N/A

Bugs Fixed

• The PT-G503 Series could not upload firmware using the ABC-02 Series.

Changes

N/A

Notes

Product versions V1.0.2 and prior are compatible with all firmware versions. Product versions V2.0.0 and later are compatible with firmware V5.0 and later.

Version: v4.3	Build: Build_17090110
Release Date: Oct 18, 2017	

Applicable Products

PT-G503-PHR-PTP-HV, PT-G503-PHR-PTP-WV

Supported Operating Systems

N/A

New Features

N/A

Enhancements

- PTP: Supports BC/TC P2P/E2E.
- PTP: Supports Power profile.
- PTP: Supports 2-step to 1-step.
- IEC 62439-3: Configurable supervision frame.
- Security: Added a warning message for when the default password has not changed yet.
- Security: Encrypts security keys in the user interface.

Bugs Fixed

- Cross-site scripting vulnerability.
- Denial of Service attack vulnerability.
- Privilege escalation vulnerability.
- SSL v2/v3 vulnerability in HTTPS.
- Web console cannot be accessed when the SNMP get bulk service is running.
- Specific CLI command caused the switch to reboot with default settings.
- PTP timestamp error in announce Message.
- System rebooted after specific CLI commands.
- Telnet hangs when SSH is disabled.
- For PT-G503 models that use SFP-1G Series cannot link up with EDR-G903 models.

Changes

- Renamed RSTP transparent to RSTP Grouping.

Notes

N/A

Version: v4.2	Build: Build_17022316
Release Date: N/A	

Applicable Products

PT-G503-PHR-PTP-HV, PT-G503-PHR-PTP-WV

Supported Operating Systems

N/A

New Features

N/A

Enhancements

N/A

Bugs Fixed

N/A

Changes

N/A

Notes

N/A

Version: v4.1	Build: N/A
Release Date: N/A	

Applicable Products

PT-G503-PHR-PTP-HV, PT-G503-PHR-PTP-WV

Supported Operating Systems

N/A

New Features

• First release for PT-G503 Series.

Enhancements

N/A

Bugs Fixed

N/A

Changes

N/A

Notes

N/A