DIGI INTERNATIONAL
9350 Excelsior Blvd, Suite 700
Hopkins, MN 55343, USA
+1 (952) 912-3444 | +1 (877) 912-3444
www.digi.com

Firmware Release Notes
ConnectPort LTS
Version 1.4.13 (March, 2025)

INTRODUCTION

This is a production release of firmware for the ConnectPort LTS(Linux Terminal Server) products. These devices provide serial over Ethernet connectivity for applications today and into the future. They support IPv4 and IPv6 Ethernet protocols. The ConnectPort LTS MEI product is the same size as the ConnectPort LTS (RS-232 only) and is the fastest multi-port device with a Multiple Electrical Interface (MEI) in the industry. High-end features include Telnet/SSHv2/TCP Sockets protocols, Local, RADIUS and LDAP authentication, Port logging through Local, NFS, Samba, Syslog and SD Memory cards, keyword monitoring and SMTP/SNMPv3 notification, PPP, Encrypted RealPort, Dual 10/100/1000 mbps Ethernet network interface, Python support and Digi Discovery server to allow discovery and network configuration from the Digi Discovery Tool.

SUPPORTED PRODUCTS

- ConnectPort LTS 8 Family
- ConnectPort LTS 16 Family
- ConnectPort LTS 32 Family

KNOWN ISSUES

None

ADDITIONAL INFORMATION

None

UPDATE CONSIDERATIONS

In order to add compliance with California's Senate Bill No. 327, for information privacy of connected devices, the handling of the root password for newly manufactured products is changing.

Products manufactured after January 1, 2020 will no longer use a fixed, default root password. Rather, a per-device, unique password will be assigned during manufacturing, and will be visible on a product label. It will still be possible to change the password for the root user on a per-device basis.

Admin user: The admin user is inactive in the new firmware. To activate the admin user, you must first assign a password to the admin user.

Products manufactured prior to the adoption of the new product labeling are grandfathered in and will continue to operate as before.

UPDATE BEST PRACTICES

Digi recommends the following best practices:

1. Test the new release in a controlled environment with your application before you update production devices.
2. Unless otherwise noted, apply updates in the following order:
    a. Device firmware
    b. Modem firmware
    c. Configuration
    d. Application

Digi recommends Digi Remote Manager for automated device updates. For more information, go to https://www.digi.com/products/iot-platform/digi-remote-manager. If you prefer manually updating one device at a time, follow these steps from the manual:

1. Firmware update process

TECHNICAL SUPPORT

Get the help you need via our Technical Support team and online resources. Digi offers multiple support levels and professional services to meet your needs. All Digi customers have access to product documentation, firmware, drivers, and knowledge base and peer-to-peer support forums. Visit us at https://www.digi.com/support to find out more.

CHANGE LOG

VERSION 1.4.13 March, 2025

This is a recommended release.

MD5 Checksum
8A62C4BBEE8AF21D88D3E005F44D4CF1

SHA-256
8783FB73BE911E52F2B11563907564F675726F5E15380469B882461356F47768

NEW FEATURES

None

ENHANCEMENTS

- Implement watchdog function to monitor Serial Ports and RealPort Service to reset and restart ports. [CPLTS-265]
- Write to syslog if the serial monitoring watchdog is triggered.

SECURITY FIXES

None

BUG FIXES

None

VERSION 1.4.12 October, 2024

This is a mandatory release to address security vulnerabilities.

MD5 Checksum
7F752DAA0431C210653460529F5F4A47

SHA-256
5D844889DEA46A6D1B4E7620BC0CD2FCFD21F4B0AB3676A0E45D55E666AC1D16

NEW FEATURES

None

ENHANCEMENTS

None

SECURITY FIXES

- Various web server related vulnerabilities have been closed. [SEC-4231]
    - CVE-2024-50625: Destination paths in certain POST operations not sanitized
    - CVE-2024-50626: Unauthenticated file access
    - CVE-2024-50627: Uploaded files not sanitized, leading to potential server-side code execution
    - CVE-2024-50628: Remote code execution vulnerabilities via improper handling of HTTP requests

BUG FIXES

None

VERSION 1.4.11 May, 2024

This is a recommended release.

MD5 Checksum
1D900B7CB3652C05B1BAFD16EB35A226

SHA-256

CA5A44BA57C7A9C44B9FA2A094D2153452EFCC8ABB060CF0542E8C40CF0D88EE

NEW FEATURES

None

ENHANCEMENTS

None

SECURITY FIXES

None

BUG FIXES

- Serial radio device issue. [CPLTS-267]
- Final changes for RealPort lockups. [CPLTS-260, CPLTS-264]

VERSION 1.4.10 February, 2024

This is a recommended release.

MD5 Checksum
670B632D315DB621FC423C73F0D9056D

SHA-256
622627EA356B98968372862ABCF5AF29CED29EE8B7808F794B5D4CF1310C057F

NEW FEATURES

None

ENHANCEMENTS

None

SECURITY FIXES

None

BUG FIXES

- Resolved corner case port lockup events. [CPLTS-260, CPLTS-264]
- Fixed syslog fails when specifying a socket port. [CPLTS-218]
- Fixed error when restoring from a backup config. [CPLTS-259]

VERSION 1.4.9 August, 2023

This is a recommended release.

MD5 Checksum
D7673A5A8CE11ECEAFE724E560A8B5F8

SHA-256
46E98AD0F64B15159C4439BEE3C7F54B0A96E31DDD7EA4B76ED8360F98F83BC8

NEW FEATURES

None

ENHANCEMENTS

- Serial port description now displayed in the output of “backup print”. [CPLTS-222]

SECURITY FIXES

- CVE-2022-0778 addressed with OpenSSL library updates (OpenSSL 1.1.1s) [CPLTS-213]
- CVE-2021-36767 addressed by adding ability to select a strong hash function for RealPort authentication. [CPLTS-249, CPLTS-253]

BUG FIXES

- Fixed high device CPU usage spikes. [CPLTS-236]
- Fixed “backup print” reporting of supported TLS levels in RealPort configuration. [CPLTS-245]

VERSION 1.4.8 April, 2022

This is a recommended release.

MD5 Checksum
D6ADC0E82258992015D6E4DF405B7AE3

SHA-256
8D8CFF00FD9B813D0932A1BD1B44E388332EE85BE4EDE018AB1D8B5CC60DB8C7

NEW FEATURES

None

ENHANCEMENTS

- Increased the maximum number of characters for “LDAP search base” from 32 to 256 characters. [CPLTS-194]
- Increased the maximum number of characters for “Shared secret” from 32 to 64 characters. [CPLTS-194]

SECURITY FIXES

None

BUG FIXES

- Added ability to see the bonded IP via the LCD display. [CPLTS-201]
- Output of "backup print" command now contains Ethernet Bonding configuration. [CPLTS-196]
- The 'backup print' command was not displaying NTP server configuration. [CPLTS-207]
- Fixed “WAIT_QUERY” error that occurs when changing rtstoggle settings while the port is in use. [CPLTS-197]

- Output of "backup print" command now properly displays the port profile. [CPLTS-200]
- Fixed display of incorrect baudrate on the LCD display. [CPLTS-172]

VERSION 1.4.7 March, 2021

This is a recommended release for any customer who needs the enhanced RTS functionality.

MD5 Checksum
F64BD8780A9351E886DC2793D5B0C1CB

SHA-256

C78BC609417400BAB840D3032B241D0474705627B61AEA1CFD

AE76E394B77E88

NEW FEATURES

None

ENHANCEMENTS

None

SECURITY FIXES

None

BUG FIXES

- Fixed a problem with login traps to the CLI CPLTS-187
- Fixed a problem with ALTPIN CPLTS-189

VERSION 1.4.6 November, 2020

This is a recommended release for any customer who needs the enhanced RTS functionality.

NEW FEATURES

None

ENHANCEMENTS

None

SECURITY FIXES

None

BUG FIXES

- Fixed a problem with RTS and DTR behavior CPLTS-178
- Fixed a problem with RTS Toggle CPLTS-182

VERSION 1.4.5.1 June 05, 2020

This is a mandatory release.

NEW FEATURES

None

ENHANCEMENTS

None

SECURITY FIXES

CVE-2020-8597

https://nvd.nist.gov/vuln/detail/CVE-2020-8597

pppd (Point to Point Protocol Daemon) versions 2.4.2 through 2.4.8 are vulnerable to buffer overflow due to a flaw in Extensible Authentication Protocol (EAP) packet processing in eap_request and eap_response subroutines.

Due to a flaw in the Extensible Authentication Protocol (EAP) packet processing in the Point-to-Point Protocol Daemon (pppd), an unauthenticated remote attacker may be able to cause a stack buffer overflow, which may allow arbitrary code execution on the target system. This vulnerability is due to an error in validating the size of the input before copying the supplied data into memory. As the validation of the data size is incorrect, arbitrary data can be copied into memory and cause memory corruption possibly leading to execution of unwanted code.

BUG FIXES

None

VERSION 1.4.5 November 08, 2019

This is a mandatory release.

NEW FEATURES

1. Added support for California's Senate Bill No. 327. Product manufactured after January 1, 2020 will have a unique password.

ENHANCEMENTS

None

SECURITY FIXES

Researchers have discovered new denial-of-service (DoS) vulnerabilities in Linux and FreeBSD kernels, including a severe vulnerability called SACK Panic that could allow malicious actors to remotely crash servers and disrupt communications, according to an advisory.

"The vulnerabilities specifically relate to the Maximum Segment Size (MSS) and TCP Selective Acknowledgement (SACK) capabilities. The most serious, dubbed "SACK Panic," allows a remotely-triggered kernel panic on recent Linux kernels," the advisory stated. This vulnerability also goes back a long time (since Linux v2.6.29, that was released 10 years ago).

"The issues have been assigned multiple CVEs: CVE-2019-11477 is considered an Important severity, whereas CVE-2019-11478 and CVE-2019-11479 are considered a Moderate severity".

Researchers have discovered Medium Level security fixes - Three (3) Stored XSS Scripting and one (1) unrestricted/arbitrary file upload vulnerability. We would like to provide thanks and credit to the finding of the vulnerabilities to two (2) researchers:

Murat Aydemir, Critical Infrastructe Penetration Test Specialist at Biznet Bilisim A.S

Fatih Kayran, Penetration Test Specialist

BUG FIXES

None

VERSION 1.4.4 May, 2019

- Add support for 50 Baud.
- Force HTTPS to use only TLS 1.2.
- Allow SSH client to change default password.
- Fix configuration parser to allow for non-standard characters.
- Fix to properly exit a telnet session after killing a port.
- Allow for capital letter in serial port description.

VERSION 1.4.3 Aug, 2018

- Added support to Allow access to connect as a different user (i.e. root) when logged as a normal user.

- Added a send break option.
- Added ability to disable keyboard-interactive authentication if a user has SSH publick key authentication enabled.
- Added the DHCP custom identifier option to this product.
- Updated RealPort to allow use of TLS 1.2.
- Changed network stack behavior when LTS declines/closes an additional TCP socket open request.
- Fixed typos in CLI.
- Blocked the use of Special Swedish Characters In The Serial Port Description.
- Fixed a problem where Serial port process does not start properly during boot when data is sent during boot to the port.
- Fixed a problem where we couldn't mount a Samba share from an Ubuntu 18.04 Linux server.