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 1.4.5 (November 08, 2019)

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 1.4.5 November 08, 2019

This is a mandatory release.

MD5 Checksum
714B1C1FF5DE164F94D7FEBE6118013B

SHA-256

CB9EBEE313E264E0E190ADE9D253DB754DC3224876E3060B52

DDB76C554CEE23

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.