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

Digi ConnectPort TS 8/16 Release Notes

Digi ConnectPort TS 8/16 (82001474)

Version 2.26.1 (October 2020)

INTRODUCTION

This is a production release of firmware for the Digi ConnectPort TS 8, TS 8 MEI, TS 16, TS 16 MEI and TS 16 48V.

SUPPORTED PRODUCTS

- Digi ConnectPort TS 8
- Digi ConnectPort TS 8 MEI
- Digi ConnectPort TS 16
- Digi ConnectPort TS 16 MEI
- Digi ConnectPort TS 16 48V

KNOWN ISSUES

1. Web Interface Configuration of SSH Public Key Authentication

   The device web page for “User Access” in the “Users” configuration area allows one to paste an SSH public key into a text area for use in SSH user authentication.

   Due to internal web server limitations, the text area does not handle RSA keys larger than 1024 bits.

   As a workaround, user public keys as large as 2048 bits can be pulled to the device via the command-line interface. After placing the public key file on a TFTP server:

   #> set user name={user} public_key=clear
   #> set user name={user} public_key={TFTP server IP}:{filename}

2. To eliminate potential issues with downgrade attempts this firmware will not allow negotiation of a connection with a TLS protocol version prior to 1.2. Users requiring interoperability with legacy protocol versions should not upgrade to this firmware unless they have this capability in the devices and servers they use it with.

As a result of limiting the TLS protocol, if the customer wishes to use Encrypted Realport they will need to update to a version that supports TLS 1.2. Unencrypted RealPort is not impacted. Digi is in the process of updating the currently supported Encrypted RealPort drivers so this will become possible as those releases occur. Please refer to the RealPort driver page http://www.digi.com/support/realport/ for updates and information.

UPDATE CONSIDERATIONS

1. As of 2.22.1 product defaults have changed to conform with California SB-327. See the product documentation and version history below for details.

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:
    1. Device firmware
    2. Modem/Module firmware
    3. Configuration
    4. 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.

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, knowledge base and peer-to-peer support forums.

Visit us at https://www.digi.com/support to find out more.

CHANGE LOG

2.26.1 – 82001474_R (October 2020)

This is a recommended release

SECURITY FIXES

Removed ICMP command 165 processing from network stack. This was the cause of a false positive in security scan software reporting our system as possibly vulnerable to Ripple20 after this had already been addressed.

2.25.0.1 – 82001474_P (June 2020)

This is a recommended release.

ENHANCEMENTS

A CLI configurable RADIUS timeout value has been added to avoid timeouts

associated with communication with a RADIUS server. The default timeout is three seconds.

Example usage to change the timeout for the first RADIUS server entry to a value of five seconds (timeout is in milliseconds):

```
set radius index=1 timeout=5000
```

BUG FIXES

Conditions existed in which an SSH connection to the device could allow access without username or password under very specific circumstances. This access hole has been closed.

2.24.0 – 82001474_N (April 2020)

This is a recommended release.

SECURITY FIXES

Researchers from JSOF (https://jsof-tech.com/), have found vulnerabilities within the Treck TCP/IP, IPv4, IPv6, DHCP, DHCPv6 and DNS products.

For Digi products we have rated the vulnerabilities as a high level risk. We recommend that customers immediately review and deploy the latest firmware associated with this release note to protect their devices. At time of release of this firmware, there is no known in the wild exploit of these vulnerabilities.

Digi’s internal scoring of the vulnerabilities is a CVSSv3.0 Score of 7.4. CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N

Digi will be coordinating a public disclosure of the vulnerabilities with JSOF that is tentatively set for May 14th, 2020. We are also working with the Cert Coordination Center and have been assigned VU#257161 pertaining to these issues.

Many thanks to the researchers Moshe Kol and Shlomi Oberman of JSOF for reporting these vulnerabilities.

2.22.1 – 82001474_M (November 2019)

This is a recommended release.

ENHANCEMENTS

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.

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

BUG FIXES

NA

2.21.1 – 82001474_L (September 2018)

ENHANCEMENTS

This release contains a new TLS implementation

- We now support many more modern and secure cipher suite options as well. This release provides added support for elliptic curve encryption, more hash algorithms, and block modes.
- Support for DSA keys and DSA signed certificates has been removed
- Some places where MD5 was being used as a hash have been modified to no longer use MD5 as it has been compromised. For legacy compatibility most places will still allow MD5 but users are encouraged to change this to something more secure.

BUG FIXES

NA

---

*Release Notes Part Number: 93000625
