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

Digi ConnectPort SP Release Notes

Digi ConnectPort (82002740)

Version 2.24.0 (April 2020)

INTRODUCTION

This is a production release of firmware for a limited group of the Digi Connect family of products.

The Digi Connect embedded and stand-alone device servers allow you to add web-enabled networking using a variety of connectivity options. The Digi Connect device servers provide powerful “plug-and-play”, customizable and future-safe features, and performance in one of the smallest solutions available.

SUPPORTED PRODUCTS

- Digi Connect SP MEI Python
- Digi Connect SP RS232 Python

KNOWN ISSUES

1. The unit must be power cycled for the port sharing settings to take effect.

   It is not currently possible to configure the escape characters used by client applications (connect, telnet, and rlogin).

   If the standard web service (HTTP) is disabled, the encrypted web service (HTTPS) stops operating. They will be made independently selectable in a future release.

   When attempting to upgrade the firmware on a unit which has password authentication enabled, the initial release of the firmware would fail. This current release includes a workaround to this behavior by allowing the user to disable passwords during the time period of the firmware upgrade.

   In order to clear the persistent configuration storage from the CLI one can execute the “boot action=factory” command. The only web accessible method for clearing the storage is available via the reset functionality in the administrative pages at “admin/factory_defaults.htm”.

When attempting to replace files in the file system, simply overwrite the existing version of the file rather than deleting the file first. Attempting to delete the file first defeats the internal file versioning maintained by the firmware, and can confuse your browser's cache.

For the most consistent experience with the user interface, it is suggested that you clear your Internet cache.

Microsoft Internet Explorer 6 Service Pack 1 (SP1) has a known problem where it displays the error message "Internet Explorer Cannot Open" when you use an HTTPS URL to access this Digi product. The following Microsoft article explains the problem:

`http://support.microsoft.com/default.aspx?kbid=812935`

Digi devices do not support SSL renegotiation. This can cause problems with some Open SSL applications that do not correctly handle this situation. To work around this problem, use the "openssl -quiet" option.

There is no IPV6 support for IA (Industrial Automation) or Modem Emulation.

TFTP using IPv6 addresses is not supported.

Backup using IPv6 addresses is supported using the Web UI but not

CLI.

Downgrading a unit from an IPv6-enabled EOS to an IPv4-only EOS will result in the loss of some IP address settings. To insure that settings are not lost in this situation, a user is advised to do a back-up of their device prior to upgrading it to an IPv6-enabled EOS. If, after upgrading, a user wishes to go back to an IPv4-only EOS, they should:

o Upload the IPv4-only EOS to the device o Revert the device to factory defaults o Restore the device using the saved backup configuration

The IA route option "set ia route connect={active|passive}" is not supported in this release. Contrary to what is stated in the Command Reference manual, connect cannot be set to active.

Setting the Serial Profile to Industrial Automation only works smoothly if you have NOT set IA parameters manually by Telnet or command line. Use one method only - either Web UI or Telnet.

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.

   Our password hashing algorithm includes a key-stretching portion to make brute-force attacks more costly. This algorithm in our new security code has more overhead and login will now take more time (3-8 seconds).

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

2.24.0 – 82002740_T (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 – 82002740_S (January 2020)

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

- DCSP-26: A memory leak related to SSL/TLS was eliminated in this release.

2.21.1 – 82002740_R (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: 93001330