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

Digi ConnectPort X2D Release Notes

Digi ConnectPort X2D (82002549)

Version 2.26.1 (October 2020)

INTRODUCTION

These are the release notes for the Digi ConnectPort X2D.

The ConnectPort X2D gateway uses a Digi Connect ME 9210 module with 8 MB of Flash, and 16 MB of RAM.

The ConnectPort X2D gateway provides support for communication to end nodes in a wireless PAN from a parent application running on an IP network. The behavior of the gateway can be customized through the Python development environment.

This firmware can support applications that require communicating directly with the wireless PAN module in the ConnectPort X2D gateway via RealPort, Modbus, or UDP/TCP sockets.

SUPPORTED PRODUCTS

- Digi ConnectPort X2D
- Digi ConnectPort X2D 9XTend

KNOWN ISSUES

None

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 – 82002549_K (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.

2.24.0 – 82002549_J (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 – 82002549_H (December 2019)

This is a recommended release.

SECURITY FIXES

1. Changes for California SB-327

   In order to comply with regulations in the state of California (SB-327), this firmware now supports being manufactured with a unique per-device password. Existing products manufactured prior to this change will continue to default to the prior fixed value ‘dbps’ but will be impacted by changes to defaults that have been made.

   When applicable, this password is the initial factory default value for the ‘root’ and ‘custom’ users and the Digi Device Discovery (ADDP) tools and can be found printed on a label attached to the product. As always, Digi recommends that users take the opportunity to change the passsword to a value known only to themselves when performing the initial configuration of the product.

   - The default factory settings for login suppression have changed. All products will require login out of the box.

     The prior behavior can be recovered in the CLI with newpass command and providing an empty string when prompted or in the WebUI on the Configuration->Security page by un-checking and applying the “Enable password authentication” checkbox.

   - SNMP has been disabled in the factory defaults. Prior behavior can be recovered with the ‘set service’ command in the CLI or in the Configuration->Network->“Network Services Settings” page in the WebUI.

2. 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.

   - Certificates and certificate requests generated by the product will now be signed with a SHA256 hash.

---

*Release Notes Part Number: 93000716