DIGI INTERNATIONAL
9350 Excelsior Blvd, Suite 700
Hopkins, MN 55343
952-912-3444 / 877-912-3444
www.digi.com

To: All Customers
From: Digi Security Team
Date: 08/25/2023
Subject: RealPort CVEs

This document includes vulnerability findings from a report that Dragos submitted. Below are the CVEs that Dragos reported to us, Digi International. Listed below is a table of Digi International products that were reported as vulnerable by Dragos.

Concern raised: CVE-2021-36767
Digi's response: This CVE is not applicable to DAL devices running 21.11 or newer firmware. The ConnectPort LTS is not vulnerable due to the device not supporting the challenge/response authentication. Support is being added for this feature in the next release and will include the same fix as other implementations. The ConnectPort TS 8/16 and Connect ES are vulnerable to this CVE and will receive an update on August 30th with the release of NDS version 2.26.2.4.

Concern raised: CVE-2021-35977
Digi's response: This vulnerability was fixed in Windows RealPort driver version 4.10.490.

Concern raised: CVE-2021-35979
Digi's response: This vulnerability was fixed in Windows RealPort driver version 4.10.490. Certificates for TLS connections are now pinned when the first encrypted connection is established. The device must then present the same certificate on each subsequent connection, or the connection will be rejected, and a message will be sent to the event log.

Concern raised: CVE-2023-4299
Digi's response: The fix was to enforce an order where the device would not respond to a challenge until the client successfully authenticates itself. This vulnerability was fixed in DAL version 21.11 and later. The ConnectPort TS 8 MEI, ConnectPort TS 8/16, and Digi Connect ES are vulnerable and will receive an update on August 30th with the release of NDS version 2.26.2.4.

Digi International Products	Vulnerable/Fixed
RealPort software for Windows, version 4.8.488.0 and earlier	• CVE-2021-35977 **Fixed in 4.10.490** • CVE-2021-35979 **Fixed in 4.10.490**

RealPort software for Linux, version 1.9-40 and earlier	• CVE-2021-35977 **Vulnerable, less critical** • CVE-2021-35979 **Vulnerable, less critical**
Digi ConnectPort TS 8/16, all versions	• CVE-2021-36767 **Fixed in firmware version 2.26.2.4, August 30th** • CVE-2023-4299 **Fixed in firmware version 2.26.2.4, August 30th**
Digi Passport Console Server, all versions	• Fix is not feasible
Digi ConnectPort LTS 8/16/32, all versions	• CVE-2021-36767 **Fixed in version 1.4.9, August 30th**
Digi CM Console Server, all versions	• EOL no update planned
Digi PortServer TS, all versions	• Fix is not feasible
Digi PortServer TS MEI, all versions	• Fix is not feasible
Digi PortServer TS MEI Hardened, all versions	• Fix is not feasible
Digi PortServer TS M MEI, all versions	• Fix is not feasible
Digi 6350-SR, all versions	• Does not contain RealPort
Digi PortServer TS P MEI, all versions	• Fix is not feasible
Digi One IAP Family, all versions	• Fix is not feasible
Digi One IA, all versions	• Fix is not feasible
Digi One SP IA, all versions	• Fix is not feasible
Digi One SP, all versions	• Fix is not feasible
Digi WR31, all versions	• EOL no update planned
Digi WR11 XT, all versions	• EOL no update planned
Digi WR44 R, all versions	• EOL no update planned
Digi WR21, all versions	• EOL no update planned
Digi Connect ES, all versions	• CVE-2021-36767 **Fixed in firmware version 2.26.2.4, August 30th** • CVE-2023-4299 **Fixed in firmware version 2.26.2.4, August 30th**
Digi Connect SP, all versions	• EOL no update planned
Digi ConnectCore 8X products, all versions	• Does not contain Realport

Thank you,
Digi International Security Team