Product Change Notice	Date May 21, 2020
Product	Connect ES, SP, ConnectPort TS, X4, X2, certain AnywhereUSB products

Audience	All Digi partners/customers
Product Notice	This is an update to previously issued PCN#200427-03 that was sent April 27th, 2020. This includes updates to announcement dates and vulnerability level. Change are shown in red. Digi International's security team was recently contacted by an independent security research company, JSOF, concerning vulnerabilities found in some Digi products. In working with the researchers, we were able to narrow down the vulnerabilities to a third party library we use within our products made by a company called "TRECK". These third party libraries provide the network (TCP/IP, IPv4, IPv6) stack in our products. In reviewing these vulnerabilities, US-Cert and Miter have classified the highest level as a possible "critical" severity (CVSS v3.1 score 10.0) vulnerability (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H). Some of these vulnerabilities can be triggered remotely without any authentication on the device. The vulnerability can lead to a full remote code execution on the target device. CVE's have now been assigned to these issues. Digi has fixed the vulnerabilities within the software, and have made it available in firmware releases beginning in April of 2020. These firmware versions are now available to our customers. We strongly recommend that you update to the latest version of your product's firmware to eliminate these potential risks. Please visit the support section of Digi's website to download the latest firmware release for your products. Digi International will be coordinating a public disclosure of the vulnerabilities with JSOF and TRECK that is tentatively set for June 15th, 2020. We are also working with the US-CERT and VU#257161 has been assigned for this vulnerability. The following CVE's have now been assigned: CVE-2020-11896, CVE-2020-11897, CVE-2020-11898, CVE-2020-11899, CVE-2020-11900, CVE-2020-11901, CVE-2020-11902, CVE-2020-11903, CVE-2020-11904, CVE-2020-11905, CVE-2020-11906, CVE-2020-11907, CVE-2020-11908, CVE-2020-11909, CVE-2020-11910, CVE-2020-11911, CVE-2020-11912, CVE-2020-11913, CVE-2020-11914

	Information will be posted on Digi's website at https://www.digi.com/security when details of this vulnerability are released. Digi is committed to keeping our products secure through the life cycle of our products. If you have questions on the security of our products, feel free to discuss this with our technical support hotlines. If you know of vulnerabilities and would like to report security issues, feel free to send email to security@digi.com and follow our vulnerability reporting program as listed on our website at https://www.digi.com/security. Digi would like to thank the researchers Moshe Kol and Shlomi Oberman of JSOF https://jsof-tech.com/.

Affected Products	The following product families are impacted: Connect ES, Connect SP, ConnectPort TS, Connectport X4, ConnectPort X2, Certain AnywhereUSB products (Anywhere USB Plus are not affected). Products with 2MB flash are not affected by the Treck vulnerability, as they contain the Fusion stack. A separate notice is being issued for Embedded/OEM products

Timing of Change	Firmware images for the listed products have been released to the Product Support section of the Digi web site. Customers are directed to update as soon as possible.

Authorization	Digi Product Management

SKU	**Description**
X2-HMA-EM-W	CPX2 DM900HP Ethernet AU3
X2-HMU-EM-A	CPX2 900HP Ethernet
X2-HMU-EM-B	CPX2 900HP Ethernet Brazil
X2-Z11-EM-A	ConnectPort X2 ZB Ethernet 9210 w/Python 8/16
X2-Z11-EM-W	ConnectPort X2 ZB Ethernet 9210 8/16 Int
X4-HMU-U901-A	CPX4 DM900HP HSPA+ US
X4H-Z1U-B101-US	ConnectPort X4H ZB 1XRTT Sprint
X4H-Z1U-L301-US	CPX4H ZB LTE US
X4-P8J-U901-W	CPX4 868 HSPA+ Int

X4-Z11-E-A	CPX4 ZB US
X4-Z11-E-W	CPX4 ZB Int
X4-Z11-PE-A	CPX4,IA ZB US
X4-Z11-PE-W	CPX4,IA ZB Int
X4-Z1J-U901-CW	CPX4 ZB HSPA+ Int China
X4-Z1J-U901-W	CPX4 ZB HSPA+ Int
X4-Z1U-U901-A	CPX4 ZB HSPA+ US
X4-Z1U-U905	CPX4 IA ZB HSPA+ US
70002323	ConnectPort TS 8
70002329	ConnectPort TS 8 MEI
70002388	ConnectPort TS 16
70002534	ConnectPort TS 16 MEI
70002538	ConnectPort TS 16 48VDC
70002543	ConnectPort TS 8 MEI
AW-TS-44	AnywhereUSB TS
AW-USB-14	AnywhereUSB/14
AW-USB-2	AnywhereUSB/2
AW-USB-5	AnywhereUSB/5 Gen2
AW-USB-5M	AnywhereUSB/5 MHC
DC-ES-4SB-EU	Connect ES 4 SB EU
DC-ES-4SB-SW-EU	Connect ES 4,4+1 SB EU
DC-ES-8SB-EU	Digi Connect ES 8 SB EU
DC-ES-8SB-SW-EU	Connect ES 8,4+1 SB EU
DC-SP-01-S	Connect SP -S Worldwide