Product Change Notice	Date May 22, 2020
Product	ConnectCore 9C, 9P, Connect EM,ME,WME, SP NetSilicon 7520, 9210,9215,9360, 9750 (with NET-OS and NDS(PlugNPlay) operating systems)

Audience	All Digi partners/customers
Product Notice	This is an update to previously reissued PCN #200427-02 that was sent out on April 27th, 2020. Updates to announcement dates and how to handle older software revisions. (Changes in Red) Digi International's security team was recently contacted by an independent security research company, JSOF concerning vulnerabilities found in some of 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 as well: 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 Kool and Shlomi Oberman of JSOF Tech.

Affected Products	The following product families are impacted: ConnectCore 9C, 9P, Connect EM,ME,WME, SP NetSilicon 7520, 9210,9215,9360, 9750 *See attached list

Notes/Actions	**NET-OS:** Patches for NET+OS 7.5 are available for download through the Digi ESP Package Manager.Customers are encouraged to install the **TCPIP_Updates_752** package, rebuild the firmware and update their products with the patched firmware. The Treck vulnerability does not affect NET+OS 6 versions and earlier. If upgrading from 7.4.2, GNU tools will replace Green Hill tools. **NDS(PlugNPlay)**: Firmware images for the listed products have been released to the Digi web site in the Product Support section. Customers are directed to update as soon as possible. The Treck vulnerability does not affect 2MB Flash product, as they use the Fusion stack. **Questions:** Please contact your Digi Sales Representative or Technical Support team via email at tech.support@digi.com

Timing of Change	Firmware images for the listed products will be available on 4/27/20. Customers are directed to update as soon as possible.

Authorization	Digi Product Management

SKU	Description
CC-9C-V212-Z1	CC9C 4NR/16 8/D
CC-9P-T225-Z1	CC9P9360,32ND/32MB,NS9360,177MHz,RTC
CC-9P-T236-Z1	CC9P9360,64ND/64MB,177MHz,0-70Â°C
CC-9P-V236-Z1	CC9P9360,64ND/64MB,NS9360,155MHz,RTC
CC-9P-V502-C	CC 9P 9215 4/8 NET+OS no ENET
CC-9P-V513-C	CC9P9215,8NR/16MB NET+OS, ENET,150MHz
CC-9P-V524-C	CC9P9215,16NR/32MB NET+OS, ENET,150MHz
DC-EM-02T-C	Connect EM -C LED Header 10V FLASH
DC-EM-02T-NC	Digi Connect EM NC CF/W
DC-EM-02T-S	Digi Connect EM POP 10V FLASH
DC-ME-01T-C	Connect ME CF/W NG
DC-ME-01T-PC	Connect ME -C NG 802.3af
DC-ME-01T-PS	Connect ME -S 802.3af
DC-ME-01T-S	Connect ME SF/W NG
DC-ME4-01T-C	Connect ME -C 4MB Flash
DC-ME4-01T-S	Connect ME -S 4MB Flash
DC-ME-9210-NET	Connect ME 9210 4/8 -C JTAG
DC-ME-Y401-C	Connect ME 9210 2/8 -C
DC-ME-Y402-C	Connect ME 9210 4/8 -C
DC-ME-Y402-S	Connect ME 9210 4/8 -S 10v
DC-ME-Y413-C	Connect ME 9210 8/16 NET+OS
DC-SP-01-C	Connect SP -C MEI noPOE noJTAG
DC-WME-Y402-C	Connect Wi-ME 9210 b/g 4/8MB NET+OS
NS7520B-1-C36	36MHZ,COMMERCIAL TEMP
NS7520B-1-C55	55MHZ,COMMERCIAL TEMP
NS7520B-1-I46	46MHZ,INDUSTRIAL TEMP
NS7520B-1-I55	55MHZ,INDUSTRIAL TEMP
NS9210B-0-I75	NS9210, 75MHZ, -40 to 85C, TFBGA
NS9215B-0-I150	NS9215, 150MHZ, -40 to 85C, TFBGA
NS9215B-0-I75	NS9215, 75MHZ, -40 to 85C, TFBGA
NS9360B-0-C103	103MHz, Commercial Temp
NS9360B-0-C177	177MHz, Commercial Temp
NS9360B-0-I155	155MHz, Industrial Temp
NS9750B-A1-C200	200 MHz Commercial Temp
NS9750B-A1-I162	162 MHz Industrial Temp