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

To whom it may concern, this article includes vulnerability findings for the vulnerability, Terrapin Attack.

Vulnerability Identifier: CVE-2023-48795

Description:

Terrapin works by altering or corrupting information **transmitted in the SSH data stream** during the handshake—the earliest stage of a connection, when the two parties negotiate the encryption parameters, they will use to establish a secure connection. The attack targets the BPP, short for Binary Packet Protocol, which is designed to ensure that adversaries with an active position can't add or drop messages exchanged during the handshake. Terrapin relies on prefix truncation, a class of attack that removes specific messages at the very beginning of a data stream.

To perform the Terrapin attack in practice, we require MitM capabilities at the network layer (the attacker must be able to intercept and modify the connection's traffic). Additionally, the connection must be secured by either ChaCha20-Poly1305 or CBC with Encrypt-then-MAC.

The affected ciphers/MACs are:

- chacha20-poly1305@openssh.com
- hmac-sha2-256-etm@openssh.com
- hmac-sha2-512-etm@openssh.com
- hmac-sha1-etm@openssh.com

Digi International's response: Digi's Security Team reviewed this finding. Digi recommends overriding the affected ciphers/MACs until patches are released. Digi scores this vulnerability as a 4.9 https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?vector=AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N/E:P/RL:T/RC:U/CR:X/IR:X/AR:X/MAV:N/MAC:H/MPR:N/MUI:N/MS:U/MC:N/MI:H/MA:N&version=3.1. Please note that NIST has modified this CVE linked here.

OS	User Guide Link	Vulnerable Status
DAL	You can override the affected ciphers/MACs by following these steps: https://www.digi.com/resources/documentation/digidocs/90002381/Default.htm#os/services-ssh-config-t.htm?Highlight=override . *Please note, if you factory reset the device, you will lose your configuration. You will have to override the affected ciphers after a factory reset.	Vulnerable. This will be patched in DAL OS version 24.6 in June 2024. In the meantime, Digi recommends overriding the affected ciphers/MACs.
NDS		Not vulnerable
Net+OS		Not vulnerable
ConnectPort LTS	Follow these steps to modify the "sshd_config" file: https://www.digi.com/support/knowledge-base/modifying-the-sshd_config%E2%80%9D-file *Please note, if you factory reset the device, you will lose your configuration. You will have to modify the "sshd_config" after a factory reset.	Vulnerable.
Connect Sensor family		Does not use SSH.
WVA		The risk is low since SSH is not enabled by default.
Z45		The risk is low since SSH is not enabled by default.
DBL		Not vulnerable.
xOS	The upgrade path for xOS devices is to update the device to DAL firmware. The xOS-to-DAL migration instructions can be found on our Digi support site: https://hub.digi.com/support/products/cellular-routers/digi-tx64/?path=/support/asset/digi-wr64-to-tx64-migration-firmware/	Vulnerable Digi strongly suggests migrating to DAL OS.

PortServer /Digi One		Not vulnerable
SarOS		Not vulnerable
XBee 3 Cellular		Does not use SSH.