Security Advisory: CVE-2026-32746 (March 24th 2026)

Overview

Digi International has completed its review of **CVE-2026-32746** and has determined that Digi's products and services are **not affected** by this vulnerability.

This vulnerability has been reported as affecting GNU Inetutils `telnetd`. Digi reviewed its products and services for exposure and determined that no Digi products or services are impacted.

Digi Products and Services

Digi has determined that the following product families and services are not affected by CVE-2026-32746:

Product Category	Product/Service	Status
Cellular/Ventus (Cellular/Networking)	Digi EX Family	Not affected
	Digi IX Family	Not affected
	Digi Remote Manager Digi On-Prem Manager	Not affected
	Digi TX Family	Not affected
	Ventus/Genesis	Not affected
OEM (Embedded Systems)	ConnectCore Family	Not affected
	ConnectCore 8M Mini	Not affected
	ConnectCore 8X	Not affected
	ConnectCore 8X SBC Pro	Not affected

	Digi Embedded Android	Not affected
	Digi HX15 Gateway Family	Not affected
	Digi HX20 Gateway Family	Not affected
	Digi XON	Not affected
	older NDS/GeneOS products (ConnectPort X4, etc.)	Not affected
	XBee 3 Cellular	Not affected
	Xbee Zigbee Gateway	Not affected
	XBee Gateway	Not affected
	XBee Hive	Not affected
	XBee Hive Border Router	Not affected
	XBee RF Family (long and short)	Not affected
	XBee SX	Not affected
	XBee Wi-Sun	Not affected
	XBee XR	Not affected
	XBee-PRO	Not affected
	Particle	Not affected
IM (Cellular/Networking)	Connect Sensor+ Family	Not affected
	Digi AnywhereUSB Manager	Not affected

	Digi AnywhereUSB Plus Family	Not affected
	Digi Axess	Not affected
	Digi Connect EZ Family	Not affected
	Digi Connect IT Family	Not affected
	Digi ConnectPort LTS Family	Not affected
	Digi Navigator	Not affected
	Digi PortServer Family	Not affected
	Digi Realport	Not affected
	Edgeport Family	Not affected
	Hubport Family	Not affected
	Z45 Industrial Controller Family	Not affected
Opengear	ACM7000 Resilience Gateway	Not affected
	CM7100 Console Server	Not affected
	CM8100 Console Server	Not affected
	IM7200 Infrastructure Manager	Not affected
	OM1200 Operations Manager	Not affected
	OM2200 Operations Manager	Not affected

	Lighthouse	Not affected
SmartSense	B2 Sensor	Not affected
	B3 Sensor	Not affected
	BZ Gateway	Not affected
	Cloud Dashboard	Not affected
	Jolt Products	Not affected
	NIST Probes	Not affected
	Sensor Hub	Not affected
	Smart Shield	Not affected
	SmartLink	Not affected
	T1 Sensor	Not affected
	Z Sensor	Not affected
IT	IT services	Not affected
	Professional Services	Not Affected

Impact Summary

According to public reporting, **CVE-2026-32746** is a buffer overflow in the GNU Inetutils `telnetd` LINEMODE SLC handler that may allow memory corruption during Telnet option negotiation.

Public sources describe this issue as network-reachable over **TCP port 23**, exploitable **without authentication**, and potentially leading to **remote code execution with root privileges** on affected systems.

Digi has completed its assessment and determined that Digi products and services are not affected.

Digi International Response

Our security and engineering teams completed a review of Digi's products and services that could incorporate the affected component.

Based on that analysis, Digi determined that no products or services are affected by this vulnerability. No remediation action is required for Digi offerings.

Customer Guidance

No customer action is required for Digi's products and services related to this vulnerability.

Customers should continue to follow general security best practices in their own environments, including disabling Telnet where it is not required and limiting exposure of externally accessible services.

Status and Updates

This advisory will be updated if new information becomes available.

Contact Information

For questions or concerns, customers may contact Digi International Customer Support or their designated account representative.