Security Advisory: React Server Components / Next.js Vulnerability (December 2025)

Overview

On December 3, 2025, a critical industry-wide vulnerability was disclosed involving React Server Components (RSC) and certain versions of Next.js (CVE-2025-55182 / CVE-2025-66478). The issue has been classified as a **Remote Code Execution (RCE)** vulnerability with the highest severity rating (CVSS 10.0). This vulnerability exists in the underlying open-source components used across many modern web frameworks.

Digi International confirmed potential impact across our product and service portfolio (confirmed as low), and immediately patched affected systems. Our internal security processes remain fully engaged, and our teams have verified all components that rely on React or Next.js. Because we maintain regular update and patch cycles across our systems, our exposure to this vulnerability is minimal.

Digi Products and Services

Org	Product/Service	Status
Cellular and Networking	Ventus/Genesis	not affected
	Ventus/Implementation Group	not affected
	Digi Remote Manager	Affected; Digi Remote Manager has been patched.
	Digi On-Prem Manager	not affected
	Digi TX Family	not affected
	Digi IX Family	not affected
	Digi EX Family	not affected
	Digi Axess	not affected
	Digi Navigator	not affected
	Digi AnywhereUSB Manager	not affected
	Digi AnywhereUSB Plus Family	not affected
	Connect Sensor+ Family	not affected

	Connect Sensor XRT-M	not affected
	Z45 Industrial Controller Family	not affected
	Hubport Family	not affected
	Digi Connect EZ Family	not affected
	Digi Connect IT Family	not affected
	Edgeport Family	not affected
Embedded Systems (OEM)	XBee 3 Cellular XBee Hive Xbee Hive Border Router XBee Gateway older NDS/GeneOS products- (ConnectPort X4/X2) XBee Wi-Sun XBee XR XBee SX XBee-PRO	not affected
	XBee RF (long and short)	not affected
	ConnectCore	not affected
	Digi XON	not affected
	Digi HX15 Gateway Family	not affected
	Digi HX20 Gateway Family	not affected
Opengear	OM2200 Operations Manager	not affected
	CM8100 Console Server	not affected
	ACM7000 Resilience Gateway	not affected
	OM1200 Operations Manager	not affected
	IM7200 Infrastructure Manager	not affected
	CM7100 Console Server	not affected
	Lighthouse	not affected
Smartsense	Cloud Dashboard	not affected
	T1 Sensor	not affected
	Z Sensor	not affected
	B2 Sensor	not affected

	B3 Sensor	not affected
	NIST Probes	not affected
	Sensor Hub	not affected
	BZ Gateway	not affected
	Smart Shield	not affected
	SmartLink	not affected
	Jolt	not affected
IT	Professional Services	not affected
	IT services/systems	1 system affected and has been patched

Impact Summary

This vulnerability may allow an attacker to execute arbitrary code on affected systems by exploiting unsafe deserialization routines in React Server Components.

There is currently **no evidence of any compromise or malicious activity** within Digi International systems.

The vulnerability is present in specific upstream open-source packages. Digi's completed analysis confirms that exposure within our environment is limited and low-risk, and all identified affected components have already been patched.

Digi International Response

Our security and engineering teams have completed a comprehensive analysis of all Digi products and services that could incorporate the affected components.

All relevant vendor-provided patches and updates have been applied, and any required remediation steps are complete.

Continuous monitoring remains in place to detect any abnormal or suspicious activity related to this vulnerability.

We will update this advisory if new information becomes available, but no additional impact is currently expected.

Customer Guidance

At this time, **no customer action is required**.

Digi International has:

- Identified and reviewed all products and services potentially affected
- Applied all necessary patches and remediation steps
- Verified that no customer-facing risk remains

Customers concerned about their own environments should review their use of React 19.x or Next.js 15.x/16.x and apply patches provided by the React and Next.js maintainers.

Status and Updates

This advisory is updated as new information emerges. Please check back regularly for the latest details.

Contact Information

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