Security Advisory: PHP2Shell (CVE-2026-109618 and CVE-2026-109619) PHP Remote Code Execution Vulnerabilities

Oct 30, 2026

Overview

Digi International is aware of two critical vulnerabilities in the PHP scripting language, collectively referred to as "PHP2Shell," that were publicly disclosed on 21 October 2026. Digi's engineering and security teams are inventorying and scoping Digi products, services, and hosted systems to determine whether any are affected.

This advisory will be updated as the investigation progresses, including a list of affected products and patched firmware versions where applicable.

Vulnerability Details

PHP2Shell refers to two flaws in PHP's core request and memory handling. Each can allow an unauthenticated remote attacker to execute arbitrary code on a server running a vulnerable version of PHP, without requiring any flaw in the application code running on top of it.

- **CVE-2026-109618:** an out-of-memory condition can interrupt PHP while the internal data for a request is only partially initialized, leading to memory corruption and remote code execution.
- **CVE-2026-109619:** internal request state is not reset before its underlying memory is released. A later request handled by the same worker can use the stale data (use-after-free), leading to remote code execution.

Exploit code has been publicly released, and exploitation attempts have been reported in the wild.

CVE Identifiers

This issue is tracked under the following CVE IDs. Full details can be found in the NVD entries: CVE-2026-109618 and CVE-2026-109619.

Both were reported at a CVSS v4.0 base score of 9.2 (Critical).

Products and Services

We are still inventorying and scoping our product and services lineup. This section will be updated with the results as time goes on.

Product Category	Product/Service	Status
MSBU (Cellular/Ventus)	Digi EX/IX/TX Family	Not affected.
	Digi xOS	Not affected.
	Digi Remote Manager (Digi RM)	Not affected.
	Digi On-Prem Manager (DOM)	Not affected.
	ARMT	Not affected.
	Ventus Genesis	Not affected.
	Ventus OS	Not affected.
Particle/OEM (Embedded Systems)	Digi Embedded Android	Investigating.
	Digi Embedded Yocto (DEY)	Not affected.
	ConnectPort Products	Not affected.
	Digi HX15 Gateway Family	Not affected.
	Digi HX20 Gateway Family	Not affected.
	Digi XON	Not affected.
	NDS/GeneOS products	Not affected.
	Xbee Zigbee Wi-Fi Hub	Not affected.
	Xbee Industrial Gateway	Not affected.
	XBee 3 Cellular	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.
	XBee Studio	Not affected.
	XCTU	Not affected.
	Particle Embedded Devices	Not affected.
	Particle Tachyon	Not affected.
	Particle Cloud	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 Axess Mobile App	Not affected.
	Digi Connect EZ Family	Not affected.
	Digi Connect IT Family	Not affected.
	Digi Connect WS	Not affected.
	Digi ConnectPort TS Family	Not affected.
	Digi ConnectPort LTS Family	Investigating.
	Digi Navigator	Not affected.
	Digi PortServer Family and Digi One	Investigating.
	Digi Realport	Not affected.
	Edgeport Family	Not affected.
	Hubport Family	Not affected.
	Z45 Industrial Controller Family	Not affected.
Opengear	ACM7000 Resilience Gateway	Not affected.

		https://portal.opengear.com/customerservice/s/article/Security-Advisory-CVE-2026-109618-and-CVE-2026-109619
	CM7100 Console Server	Not affected. https://portal.opengear.com/customerservice/s/article/Security-Advisory-CVE-2026-109618-and-CVE-2026-109619
	CM8100 Console Server	Not affected. https://portal.opengear.com/customerservice/s/article/Security-Advisory-CVE-2026-109618-and-CVE-2026-109619
	IM7200 Infrastructure Manager	Not affected. https://portal.opengear.com/customerservice/s/article/Security-Advisory-CVE-2026-109618-and-CVE-2026-109619
	OM1200 Operations Manager	Not affected. https://portal.opengear.com/customerservice/s/article/Security-Advisory-CVE-2026-109618-and-CVE-2026-109619
	OM2200 Operations Manager	Not affected. https://portal.opengear.com/customerservice/s/article/Security-Advisory-CVE-2026-109618-and-CVE-2026-109619
	Lighthouse	Not affected. https://portal.opengear.com/customerservice/s/article/Security-Advisory-

		CVE-2026-109618-and-CVE-2026-109619
Smartsense/Jolt	B2 Sensor	Not affected.
	B3 Sensor	Not affected.
	BZ Gateway	Not affected.
	Cloud Dashboard	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.
	Jolt Products and Services	Affected; Remediation completed.

Support and Questions

If you have any questions or require assistance, please contact our support team at https://www.digi.com/support. We appreciate your attention to this matter and thank you for your continued trust in Digi International.