

PRODUCT SECURITY ADVISORY

October 22, 2026

PSIRT Record Number
TEK-PSA-003-1022

OVERVIEW

Two critical PHP vulnerabilities were published on October 21, 2026. Together these are referred to as PHP2Shell.

- CVE-2026-109618 - Critical PHP vulnerability remote control execution via out of memory corruption.
- CVE-2026-109619 - Critical PHP vulnerability remote control execution via stale global state.

PSIRT STATEMENT

Tektronix has identified impacted versions of PHP in the 3 Series MDO, 4 Series B MSO, 5 Series B MSO, 5 Series MSO Low Profile, 6 Series B MSO, 6 Series Low Profile Digitizer, and 7 Series DPO. This applies to both Windows and non-Windows versions of the products. We have not yet confirmed if the vulnerabilities are exploitable in these products.

Tektronix continues to investigate these vulnerabilities and their potential impacts on all Tektronix products and will update this advisory as needed.

Tektronix is working on providing updated firmware with patched versions of PHP for all affected products. As a temporary mitigation, we recommend physically disconnecting the device from any untrusted network.

You should always follow your company's security practices. In addition, these general practices may also enhance security for Tektronix's products:

- Only operate Tektronix products in protected or secure networks, limiting remote access.
- When remote access to Tektronix products is required, use only secure remote access methods (for example, your organization's VPN or other secure method)
- In accordance with your organization's security policy and/or industry best practices and recognizing that VPNs may also have vulnerabilities and should be updated to the most current version available.
- As with any device, segment or isolate Tektronix products from your business network, whenever possible.
- Take additional mitigation steps outlined in CERT vulnerability notice #257161 as appropriate.

ABOUT TEKTRONIX PRODUCT SECURITY

Tektronix helps our customers innovate solutions accurately, safely, and securely. Tektronix is committed to developing secure solutions for our customers.

The Product Security Incident Response Team (PSIRT) focuses on identifying, assessing, and analyzing risks associated with security vulnerabilities within Tektronix products. The Tektronix PSIRT is a diverse team of subject matter experts responsible for delivering best in class support to contain and minimize the vulnerability impact.



For more information about Tektronix Product Security and PSIRT, please visit us at <https://tek.com/en/support/product-security/advisories>

You may also contact us at PSIRT@tektronix.com.

Initial Publication Date	Last Published Date
[10/22/2026]	[10/22/2026]