PHP2Shell Vulnerability Guidance for 10ZiG Endpoints and 10ZiG Manager v5/6

Document and Version Control			
Version	Created by	Date	Authorised & Checked
1.0	Ed Richardson	10/31/2026	ER

10ZiG Technology has completed its assessment of CVE-2026-109618 and CVE-2026-109619 (PHP2Shell).

We can confirm that 10ZiG Manager v5 and v6 are not impacted. Standard 10ZiG Windows 10 IoT and Windows 11 IoT OS images are also not impacted. Customers using customized Windows images are encouraged to perform their own vulnerability scan to confirm PHP or other affected components have not subsequently been installed outside the factory default image.

10ZiG Linux OS versions up to and including v16.6 contain an affected PHP version.

The updated PHP module will be integrated natively into ongoing firmware planned from 16.6.1.4 onwards which will be available week commencing October 26th 2026.

In the vast majority of deployments, 10ZiG endpoints will not be directly exposed to the public Internet, significantly limiting exposure to these vulnerabilities. Customers wishing to fully remove the identified network attack surface can additionally disable inbound access to ports 80 and 443, preventing network access to the lighttpd/PHP service. This is performed via the client configuration - Security Settings applet either remotely via 10ZiG Manager or locally under Control Panel.

Disabling these inbound services does not impact 10ZiG Manager communication, as management communication is securely established by the endpoint as an outbound connection over port 443 using the 10ZiG Secure Agent.

10ZiG recommends customers apply the updated PHP module using firmware 16.6.1.4 or higher at the earliest opportunity.