# NIGC Tech Alert

## PHP2Shell Critical Remote Code Execution Vulnerability

The National Indian Gaming Commission recommends that tribal gaming operations immediately apply available patches to affected PHP installations, prioritizing internet-facing systems. Organizations should assess public websites, web portals, APIs, and vendor-managed applications that utilize PHP. Coordination with software vendors and managed service providers is essential to identify all affected systems and implement mitigation measures promptly, including remediation of any vulnerable API integrations.

Two critical vulnerabilities, collectively known as PHP2Shell (CVE-2026-109618 and CVE-2026-109619), may allow a remote attacker to execute arbitrary code on a vulnerable server without authentication. Both vulnerabilities have been added to the Cybersecurity and Infrastructure Security Agency (CISA) Known Exploited Vulnerabilities (KEV) Catalog, indicating active exploitation and a significant risk to affected organizations.

An attacker does not need valid credentials to exploit vulnerable systems. In many cases, simply sending a specially crafted web request to a publicly accessible PHP application may be sufficient to gain remote code execution privileges.

Consequently, tribal operations could be at risk through a vulnerable web server where attackers could:

1. Execute arbitrary commands on the server
2. Deploy malware, ransomware or web shells to your environment
3. Move laterally within your network to gain unauthorized access to sensitive patrons, employees or gaming related information
4. Disrupt gaming operations and business services

Immediate action should be taken to address all public facing applications built on affected PHP versions to remain protected from the vulnerability.

**Recommended Remediation**

1. Identify and inventory systems running any version of PHP
2. Apply the patch immediately, prioritizing internet facing systems.
3. Operations that can't update immediately, or those using PHP 8.1 or earlier unsupported versions, should take PHP based systems offline until they can be patched.
4. A web application firewall may provide some protection until systems are patched.
5. Review the official PHP security advisory for any updated guidance on patching
6. Monitor for suspicious activity, including PHP worker processes launching shells or downloading tools.

**Vendors and Third-Party Applications**

When working with vendors and third-party providers, engage with them immediately to uncover any components not visible to your administrators. Here are recommended questions when engaging with your vendors:

1. Do any of your products utilize PHP in any capacity, especially internet facing?
2. Has a security patch been released to apply to those systems?
3. What PHP version contains the fix for the PHP vulnerability?
4. Are there any compensating controls available until patches can be applied?
5. Has your company observed attempted exploitation against customers?

**Possible Vendor Actions**

When working with vendors you may want to consider requesting the following:

1. A formal statement regarding the PHPShell exposure
2. Any remediation guidance or resources
3. Patch installations procedures
4. Remediation timelines for any unsupported products
5. Verification steps demonstrating the vulnerability have been addressed

Finally, ensure you document your response actions in the form of vendor notification records, risk assessments, patch implementation dates, vulnerability scan results and evidence of the remediation. NIGC recognizes any critical control weaknesses flagged during compliance reviews or internal control assessments. Addressing these are essential to adhering to NIGC and tribal standards, protecting tribal assets, and maintaining regulatory requirements. Regardless of gaming operation, proactively maintaining critical cyber security practices will significantly reduce the risk of exploitation from attacks.

**Resources**

CISA Vulnerabilities in PHP Require Immediate Patching

National Vulnerability Database (NVD) CVE-2026-109618

We are here to help! If you suspect you have fallen victim to an attack, please inform the Division of Technology (DoT) using the iso@nigc.gov email address. If you have questions concerning any social engineering compromise or any other technical matter, please email ocio@nigc.gov.