**Nasscom-DSCI Official Media Statement**

# PHP2Shell Vulnerability: Cyber Risk Implications for Indian Ecosystem

On 21st October 2026, PHP released emergency fixes for two critical flaws, known as "PHP2Shell" (CVE-2026-109618 and CVE-2026-109619). The flaws can let an attacker run their own code on a web server without logging in. The website itself does not need to have any flaw. Researchers have shown working attacks on current versions of WordPress, Drupal, and Joomla. It is recommended to immediately update PHP now, restart the web workers and check internet-facing hosts for any compromise, from 17th October.

As of now, we are not yet aware of any Indian organization publicly reported as a victim. CERT-In has issued a vulnerability note, CIVN-2026-0510, which rates it as critical and says several reports confirm large-scale exploitation. The attacks are not aimed at any one country, so any Indian website or server that can be reached from the internet and runs an unpatched version of PHP should be treated as at risk.

## Why it Matters:

**Wide Usage:** PHP runs WordPress sites, government and university portals, small online shops, and older business systems, and many of these sit on shared hosting.

**Old Versions:** A worldwide scan by Modat found that about 79% of PHP services showing their version number run a version that PHP no longer supports. Many of these will not get a normal update.

**Data at Risk:** Attackers can steal data, deface sites, and move to other systems. One flaw can also leak passwords, tokens, and API keys from the server's memory without a full takeover. For portals hosting personal data, this is a serious risk on its own.

## What Organizations Should Do:

- **Update PHP and Restart** web servers so the fix takes effect. Updating is the only complete fix.
- **Take Unpatched Systems Offline:** Where an update is difficult, take the affected system offline.
- **Check Logs** from at least 17th October, not just from 21st October.
- **Follow CERT-In** advisories and issued guidance. Report any break-in to CERT-In.
- **Use WAF** rules and security detection mechanisms virtual patching to detect
- **Use Log Detection Mechanisms** to detect any kind of attack/threats against the PHP Services.
- **Support Clients:** Technology companies serving clients on PHP should help them address the issue.

This is a one-of-a-kind incident which can have far serious and long-term implications, if not contained promptly. How quickly our ecosystem responds to patching the vulnerability and

update will determine whether this remains a contained incident or becomes a wider national concern. DSCI is closely watching the developments across the private and public sector, guiding members and has issued threat remediation advisory to the industry."

**Attribute to: Vinayak Godse, CEO, Data Security Council of India (DSCI)**

**Read Advisory:** https://www.dsci.in/files/content/advisory/2026/PHP2Shell%20Advisory.pdf