

Critical Remote File Inclusion Vulnerability Disclosed in WordPress Core



A critical remote file inclusion vulnerability in WordPress Core permits unauthenticated attackers to execute arbitrary code by forcing page-template resolution to include local PHP files outside theme directories.

- WordPress Core contains a remote file inclusion vulnerability tracked as CVE-2026-87902
- Unauthenticated attackers can exploit page-template resolution to include arbitrary local PHP files
- Successful exploitation leads to remote code execution on vulnerable WordPress installations
- Organizations must apply vendor mitigations immediately or discontinue use if patches are unavailable
- Internet-facing WordPress assets require immediate evaluation and patching

Vulnerability Overview

The United States Cybersecurity and Infrastructure Security Agency has disclosed **CVE-2026-87902**, a critical remote file inclusion vulnerability affecting WordPress Core. The flaw permits unauthenticated attackers to manipulate the platform's page-template resolution mechanism, forcing it to include arbitrary readable local PHP files located outside the active theme directories. Successful exploitation results in **remote code execution**, granting attackers full control over vulnerable WordPress installations.

The vulnerability requires no authentication, significantly lowering the barrier to exploitation and expanding the potential attack surface for regulated institutions operating WordPress-based public portals, customer engagement platforms, or internal content management systems.

Risk to Saudi Institutions

WordPress powers a substantial portion of web infrastructure globally, including many corporate websites, customer portals, and digital service platforms operated by Saudi financial institutions, healthcare providers, and government entities. Given the unauthenticated nature of this vulnerability, internet-facing WordPress installations present immediate risk. Attackers gaining code execution capabilities can exfiltrate sensitive data, deploy ransomware, establish persistent access, or pivot to internal networks.

Regulated institutions under NCA and SAMA oversight must treat this vulnerability with urgency, particularly where WordPress installations process or store regulated data subject to PDPL requirements or handle customer-facing services.

Mitigation Guidance

Organizations must immediately apply vendor-issued security updates for all WordPress Core installations. Where patches are not yet available, institutions should implement compensating controls including restricting network access, deploying web application firewall rules, or temporarily taking vulnerable systems offline. Cloud-hosted WordPress services require coordination with service providers to confirm patching status and timelines.

What to do now

1. Conduct an immediate inventory of all WordPress Core installations across internet-facing and internal environments
2. Apply vendor-issued security patches for CVE-2026-87902 to all WordPress installations without delay
3. For systems where patches are unavailable, implement compensating controls including network segmentation, WAF rules, or temporary service suspension
4. Verify patching status with cloud service providers for externally hosted WordPress platforms
5. Review access logs and conduct forensic triage on all WordPress systems to identify potential exploitation indicators

6. Document remediation activities and timelines for compliance reporting to NCA or SAMA as applicable