

Notice to Suppliers



Critical PHP Remote Code Execution Vulnerabilities – Immediate Action Required

Originator: Kaveh Pourteymour
Job Title: Group Digital Information Officer
Business Unit: Digital & IT

NTS Number: NTS 661
Issue: 1
Date: 22 October 2026

Scope/Applicability:

All Rolls-Royce suppliers and partners.

Dear Supplier and Partners,

Introduction:

This notice requires all suppliers to **take immediate action** in response to two newly disclosed critical vulnerabilities in PHP, a technology widely used by websites, web applications and third-party products.

These vulnerabilities could allow an unauthenticated attacker to execute malicious code on an affected server. **Suppliers must immediately assess their exposure and complete all required actions below without delay.**

Affected Systems:

All PHP installations serving web requests may be affected, including:

- PHP-FPM,
- Apache with mod_php,
- php-cgi,
- FrankenPHP and
- LiteSpeed.

The risk is considered highest for Apache mod_php deployments.

Suppliers must also assess commercial products, content management systems, hosted services, appliances and other software that may include PHP as an embedded component.

Affected supported releases are:

- PHP 8.5 versions before 8.5.12
- PHP 8.4 versions before 8.4.27
- PHP 8.3 versions before 8.3.36
- PHP 8.2 versions before 8.2.35
- PHP 8.1 and earlier are end-of-life and do not receive standard updates from the PHP project.

Action Required:

1. **Identify exposure immediately.** Identify and inventory all supplier-managed or supplier-hosted systems, websites, applications and services that run or embed PHP. Prioritise systems accessible from the internet and include services delivered to, connected to, or processing data on behalf of customers.
2. **Apply security updates immediately:** Upgrade supported PHP branches to version 8.5.12, 8.4.27, 8.3.36 or 8.2.35, as applicable. For vendor-managed or bundled PHP components, apply the relevant vendor security update. Validate successful installation and service operation following deployment.
 - a. **Address unsupported versions:** Upgrade PHP 8.1 and earlier to a supported, fixed release or obtain and apply an appropriate security fix from the operating system, long-term-support or product vendor. Do not leave end-of-life installations externally exposed.
 - b. **Contain systems that cannot be patched immediately:** Remove the affected system from public access or isolate it from public networks until the fix has been applied and verified. Temporary mitigations and web application firewall controls may reduce exposure but must not be treated as alternatives to patching.
3. **Review for potential compromise:** Examine relevant web, application, endpoint, authentication and network logs for suspicious requests, unexpected processes or files, unauthorised access, outbound communications and other indicators of compromise. Preserve evidence where suspicious activity is identified.
4. **Engage relevant service providers:** Obtain confirmation from hosting providers, managed service providers and software vendors that affected services and embedded components have been assessed and remediated.
5. **Provide confirmation to Rolls-Royce:** Suppliers/partners must provide written confirmation to their Rolls-Royce point of contact that affected systems supporting the contracted service have been patched or securely isolated.

Confirmation and Incident Reporting

Suppliers must retain evidence of their assessment and remediation, including the systems reviewed, versions identified, updates applied, completion date, validation results and any approved exceptions.

Any suspected or confirmed exploitation, data compromise, service disruption or impact to systems or information associated with the contracted service must be reported immediately to Rolls-Royce Security Operations Centre (SOC): sec.reporting@rolls-royce.com. The notification must identify the affected service, known impact, containment measures, remediation status and contact details for the supplier representative responsible for ongoing coordination.

NTS Category:

General Information / Communication

Authorised by:

Kaveh Pourteymour
Group Chief Digital Information Officer