ReadiNow Response to Reported PHP Vulnerabilities (CVSS 9.2)

Last Modified on 27/10/2026 12:19 am AEDT

Summary

ReadiNow does not have exposure to this vulnerability.

Background

On 21 October 2026, security updates were released to address two critical vulnerabilities in PHP that could allow an attacker to remotely execute malicious code on vulnerable web servers, potentially resulting in unauthorised access, data theft or a compromised website. Both vulnerabilities have been rated **Critical (CVSS 9.2)**, and reports indicate that attempts to exploit them have already been observed.

ReadiNow Response

ReadiNow has promptly reviewed all code and environments. ReadiNow does not use PHP in the platform or in any supporting tools.

Update.

This bulletin was last updated on 22 October 2026

New information will be posted here if required