



# Central Depository Services (India) Limited

Convenient + Dependable + Secure

## COMMUNIQUE TO DEPOSITORY PARTICIPANTS

CDSL/IS/DP/POLCY/2026/742

October 22, 2026

### ADVISORY ON CRITICAL REMOTE CODE EXECUTION VULNERABILITIES IN PHP

This is to inform all Depository Participants that PHP is an open-source scripting language designed for server-side web development and is used to create dynamic web pages. Multiple vulnerabilities have been identified in PHP due to memory corruption and improper resource control. A remote attacker could exploit these vulnerabilities by sending specially crafted requests to the targeted system. Successful exploitation could allow the attacker to execute arbitrary code and compromise the affected system.

In this regard, all entities are advised to review the below Vulnerability Note from CERT-In regarding critical vulnerabilities affecting PHP server environments.

<https://www.cert-in.org.in/s2cMainServlet?pageid=PUBVLNOTES01&VLCODE=CIVN-2026-0510>

Please confirm in case your systems have experienced any related active exploits, anomalies, or security incidents to [dpinfosec@cdslindia.com](mailto:dpinfosec@cdslindia.com). Indicate if any End-of-Life (EOL) PHP versions are currently in use within your organization and outline the remediation measures being taken to upgrade or isolate them in context of below vulnerability note.

You may refer below relevant post from PHP.

<https://www.php.net/archive/2026.php#2026-10-21-5>

<https://thephp.foundation/blog/2026/10/21/todays-php-security-release-and-how-were-strengthening-php-security/>

Queries regarding this communiqué may be addressed to: CDSL on [dpinfosec@cdslindia.com](mailto:dpinfosec@cdslindia.com) and connect through our IVR Number 022-62343333.

**For and on behalf of**

**Central Depository Services (India) Limited**

sd/-

**Akhil Wadhavkar**

**Senior Vice President– Chief Information Security Officer**