

Security Advisory: eMudhra Certificates and PHP2Shell Vulnerabilities

PUBLISHED: October 22, 2026 | **STATUS:** No impact to FinThrive services

CURRENT STATUS

FinThrive has completed its assessment of the reported eMudhra certificate concerns and PHP2Shell vulnerabilities. FinThrive does not use eMudhra-issued certificates within its production environment. All identified systems affected by the PHP2Shell vulnerabilities have been remediated, and no evidence of exploitation has been identified within the FinThrive environment. No customer action is required.

FinThrive is aware of recent industry reports regarding eMudhra-issued certificates and the newly disclosed PHP2Shell vulnerabilities (CVE-2026-109618 and CVE-2026-109619).

As part of our ongoing security monitoring and vulnerability management processes, FinThrive assessed the potential impact of both issues across our environment. Based on our review and completed remediation activities, these issues do not pose a risk to FinThrive services or customer data.

eMudhra Certificates

STATUS: NO IMPACT IDENTIFIED

Recent reports have raised concerns regarding certain eMudhra-issued digital certificates. FinThrive does not use eMudhra-issued certificates within its production environment. Based on our review, the reported concerns related to these certificates do not impact FinThrive systems, services, or customer data.

PHP2Shell Vulnerabilities

CVE-2026-109618 and CVE-2026-109619

STATUS: REMEDIATED

The PHP Project recently released security updates addressing two critical remote code execution vulnerabilities collectively referred to as PHP2Shell.

Upon disclosure, FinThrive immediately initiated an assessment of our environment and completed remediation activities for affected systems. Our review confirmed that:

- All identified systems have been updated with the appropriate security patches.
- Remediation activities were completed in accordance with established vulnerability management procedures.
- Security monitoring and validation activities were performed following remediation.
- No evidence of exploitation has been identified within the FinThrive environment.

Our Commitment to Security

Protecting customer information and maintaining the trust of our clients remain foundational to FinThrive's security program.

FinThrive continuously monitors emerging cybersecurity threats and maintains established processes for:

- Vulnerability identification and remediation
- Secure patch management
- Continuous security monitoring and threat detection
- Incident response and recovery
- Ongoing risk assessment and threat intelligence review

We will continue to evaluate emerging threats and take appropriate actions to safeguard customer data, systems, and services.

Questions?

If you have questions regarding these issues or would like additional information about FinThrive's security program, please contact your FinThrive representative or visit the [FinThrive Security and Data Trust Center](#).