Charles G. Cooper
Commissioner

TEXAS DEPARTMENT OF BANKING

2601 North Lamar Blvd., Austin, Texas 78705
512-475-1300 /877-276-5554
www.dob.texas.gov

Media Contact:
media@dob.texas.gov

INDUSTRY NOTICE 2026-05
Date: October 27, 2026

Cyber Alert – Critical Vulnerabilities Associated with Commonly Used Programming Language: PHP

As you may be aware, there have been multiple alerts regarding critical vulnerabilities associated with the programming language PHP. PHP is a commonly used server-side programming language used for many websites, content management systems, and web applications.

The Texas Department of Banking (Department) is communicating this information to ensure that your financial institution is aware of the critical vulnerabilities affecting PHP. A patch to address the known vulnerabilities was released on October 21, 2026.

The Department encourages each of its regulated entities to follow the recommended actions below to address this vulnerability.

- Identify and prioritize vulnerable assets
- Apply emergency security updates
- Implement temporary compensating controls
- Enhance monitoring and incident response

All entities should prioritize these recommended actions based on exposure, business criticality, and potential consequences of compromise. Cyber threats can evolve rapidly and require constant attention to ensure that threats are addressed promptly to protect your institution from harm.

Financial institution management and board of directors should ensure that appropriate systems are in place to readily identify and address vulnerabilities within their cybersecurity infrastructure. For more information on implementing appropriate cyber hygiene at your institution, refer to Industry Notice 2026-02: The Fundamentals of Cyber Hygiene for Financial Institutions.