Office of the
Chief Information
Security Officer
State of Texas

TLP: WHITE

Distribution Limits

TLP: WHITE = Disclosure is not limited.

The materials provided are for information only. Any recommendations are offered solely for your consideration, to the extent applicable to your circumstances.

SUBJECT: Information About Security and Vulnerability Bulletins Distributed by DIR OCISO TLP: WHITE

The Texas Department of Information Resources (DIR), Office of the Chief Information Security Officer (OCISO) endeavors to provide the information security community with timely and actionable security bulletins, vulnerability notifications, and relevant information to improve the security posture of the state.

Application of Potential Recommendations

Informational bulletins or vulnerability notices may be distributed for your awareness, which may not require any administrative action be taken, while others may come with recommendations that may help reduce the vulnerability of the identified system. For example, "Patch: NOW" emails often make specific recommendations based on an identified vulnerability and provide a recommended solution or mitigating configuration.

As users receive a notification for DIR OCISO, the following list identifies best practices for managing their application.

- Review the notification to determine if it is relevant to your organization. (Managed Service Provider customers, see considerations below)
- Review the software and hardware configurations to confirm applicability.
- If patches are warranted, apply any recommended patches or configurations, after appropriate testing.
    - Organizations should follow their internal change control methods, which may include vigorous testing of patches in a development environment, especially if the updated systems are external or customer facing.

- If patches cannot be applied as recommended, review notification for potentially mitigating interim steps to help reduce the system's vulnerability.
- Review pertinent system controls and configurations, including, but not limited to:
    - Applying the Principle of Least Privilege to all systems and services.
    - Running all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.

Any recommendations are offered solely for your consideration, to the extent applicable to your circumstances.

Considerations for Managed Services

Some notification recipients may have their infrastructure hosted by a Managed Service Provider (MSP). If your MSP is responsible for patch or vulnerability management, confirm the schedule and implementation of these services, whether they are scheduled during a normal maintenance window, applied as identified, or updated as requested.

For DIR Shared Technology Services (STS) customers, system level security patches and vulnerability remediations are regularly performed based on the specific platform's schedule. You can use the STS Portal to request your platform's information, review reports, or submit tickets.

Texas ISAO Notifications

The Texas Information Sharing and Analysis Organization, (Texas ISAO) provides a mechanism for state and non-state entities in Texas to share actionable and timely information regarding cybersecurity threats, best practices, and remediation strategies, while advancing the cybersecurity capabilities and resilience of the State of Texas. For additional information, subscribe to sector specific notification lists, submit a threat report, or view available security documentation, visit isao.texas.gov.

The Texas ISAO includes partnerships with non-DIR entities that may also send out security and vulnerability bulletins. These notifications are provided for information only, and the views and opinions expressed are their own and do not necessarily reflect those of DIR or its employees.

Subscription Management

Users may manage their notification subscription through the Texas ISAO webpage, the DIR Collaboration Webpage, or by referencing the original enrolment notification. Users may always contact Texas DIR OCISO at dirsecurity@dir.texas.gov with any questions.

TLP: WHITE

Sources may use **TLP: WHITE** when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject

to standard copyright rules, **TLP: WHITE** information may be distributed without restriction.
https://www.us-cert.gov/tlp

DIR.TEXAS.GOV

Assistance/Feedback/Questions?

Office of the Chief Information Security Officer
DIRSecurity@dir.texas.gov
Texas Department of Information Resources

Transforming How Texas Government Serves Texans