INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-06-22 19:03 UTC

Texas Parks and Wildlife Department Data Breach via Third-Party License System Vendor

DATA BREACH | HIGH | CVSS 7.5

SCC Item ID	SCC-DBR-2026-0195
Type	Data Breach
Severity	HIGH
CVSS Base Score	7.5
Affected Products	Texas Parks and Wildlife Department, hunting and fishing license system (via unnamed third-party vendor)
Published	2026-06-22
Discovery Source	Gemini

Executive Summary

The Texas Parks and Wildlife Department (TPWD) disclosed a breach affecting over 3 million Texas residents, originating from a cyberattack on an unnamed third-party vendor managing the state's hunting and fishing license system. The agency did not cause the breach directly; its exposure stems from a contracted service provider compromise, a supply chain risk pattern increasingly common in state government operations. Business risk includes regulatory scrutiny, civil liability, and reputational harm for any organization operating under similar third-party licensing arrangements.

Technical Analysis

TPWD's hunting and fishing license platform was compromised through its third-party vendor, consistent with MITRE ATT&CK T1199 (Trusted Relationship) and T1078 (Valid Accounts). The attack vector, malware family, and specific exploited systems have not been publicly disclosed. No CVE has been assigned. The applicable weakness classification is CWE-359 (Exposure of Private Personal Information to an Unauthorized Actor). Over 3 million individuals' personal data were exposed. The full enumeration of affected data types has not been confirmed in available public sources. The TPWD official notification at tpwd.texas.gov is the authoritative reference for data element specifics. No patch is applicable; this is a vendor-side incident requiring third-party risk and contractual remediation.

Action Checklist

1. Step 1: Containment, Identify all third-party vendors in your environment that manage state licensing, permitting, or citizen-facing data systems. Confirm whether any vendor shares infrastructure with TPWD's unnamed license system vendor. Suspend or isolate data-sharing integrations with unverified vendors pending review. Apply NIST AC-20 (Use of External Systems) to enforce connection requirements and terms.
2. Step 2: Detection, Review access logs for your citizen or customer data systems for anomalous third-party API calls, unusual bulk data exports, or credential activity associated with vendor service accounts. Monitor for indicators consistent with T1078 (Valid Accounts), off-hours logins, service accounts accessing data outside normal scope. Apply NIST AU-6 (Audit Record Review, Analysis, and Reporting) cadence. No public IOCs have been released for this incident.
3. Step 3: Eradication, No patch is available; the attack vector targeted a vendor, not TPWD systems directly. Require the vendor to provide a written incident report, root cause analysis, and remediation plan. Rotate any shared credentials or API keys between your systems and affected or similarly positioned vendors. Apply NIST IA-4 (Identifier Management) and NIST IA-5 (Authentication) for all vendor-linked service accounts. Reference CIS 5.3 (Disable Dormant Accounts) and CIS 6.2 (Establish an Access Revoking Process) to remove stale vendor access.
4. Step 4: Recovery, Validate that vendor access to your environment is re-authorized only after documented remediation. Confirm audit logging is intact and has not been tampered with per NIST AU-9 (Protection of Audit Information). Re-enable vendor integrations under enhanced monitoring. Verify CIS 8.2 (Collect Audit Logs) is enforced for all vendor-touching systems. Notify affected individuals per applicable state breach notification law if your organization holds similar data.
5. Step 5: Post-Incident, Conduct a full third-party risk assessment against all vendors with access to personal data. Establish or update vendor contracts to require breach notification timelines, security attestations, and right-to-audit clauses. Map vendor access to NIST AC-6 (Least Privilege) and AC-5 (Separation of Duties). Implement NIST AC-2 (Account Management) reviews for all vendor service accounts. Develop or update a third-party incident response playbook aligned to NIST IR controls.

IR / Forensic Enrichment

Triage Priority	URGENT
Escalation Criteria	Escalate immediately to legal counsel and executive leadership if your organization holds hunting, fishing, or outdoor recreation license data for state residents — Texas Business and Commerce Code §521.053 requires breach notification within 60 days of discovery, and exposure of over 3 million residents in the TPWD incident signals the regulatory scrutiny threshold has already been met at the state level.
Recovery Notes	Re-enable vendor integrations only after receiving and reviewing the vendor's written root cause analysis confirming the attack vector has been closed — for this breach pattern (third-party license system compromise), that means verifying the vendor has rotated all credentials, patched or replaced the compromised component, and implemented enhanced monitoring on their side. Monitor all re-established vendor API connections for anomalous bulk query behavior against citizen PII tables for a minimum of 30 days post-recovery, using query volume and off-hours access as primary indicators. Retain all incident artifacts — log exports, credential rotation records, vendor correspondence — for a minimum of 3 years to support potential regulatory review under Texas state records retention requirements.

Forensic Artifacts	API gateway or reverse proxy access logs (nginx access.log, IIS W3SVC logs, or AWS API Gateway execution logs) covering the 90-day window prior to disclosure — specifically request volume, payload size, and response row counts for vendor service account calls to citizen license data endpoints, which would show data staging or bulk exfiltration patterns | Identity provider authentication logs (Active Directory Security Event ID 4624, 4648, 4672, and 4776) for all vendor-linked service accounts — off-hours logon times, source IPs outside contracted vendor IP ranges, and privilege escalation events are the primary behavioral indicators for this valid-account-abuse breach pattern | Database query audit logs (SQL Server Profiler, PostgreSQL pg_audit, or Oracle Unified Auditing) recording SELECT statements against citizen PII tables (hunting/fishing license holder name, date of birth, address, license number) executed under vendor credentials — unusually large result sets or repeated full-table scans are the forensic signature of bulk PII harvesting | Network flow records (NetFlow, IPFIX, or firewall session logs) capturing outbound data transfer volumes from your license system database hosts to vendor-controlled IP ranges — a sudden spike in outbound bytes to a third-party SaaS endpoint, particularly over HTTPS on port 443 where content inspection is limited, is consistent with exfiltration via compromised vendor API channel | Vendor contract and access provisioning records — the absence or staleness of a security attestation, the presence of overly broad database read permissions granted to the vendor service account, and the lack of a contractual breach notification SLA are administrative artifacts that establish the control failure timeline and are essential for regulatory response and civil liability assessment

Per-Action IR Details

Step 1: Containment — Identify all third-party vendors in your environment that manage state licensing, permitting, or citizen-facing data systems. Confirm whether any vendor shares infrastructure with TPWD's unnamed license system vendor. Suspend or isolate data-sharing integrations with unverified vendors pending review. Apply NIST AC-20 (Use of External Systems) to enforce connection requirements and terms.

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 — Containment Strategy

Controls: NIST AC-20 (Use of External Systems), NIST AC-4 (Information Flow Enforcement), CIS 4.4 (Implement and Manage a Firewall on Servers)

Compensating: Export your firewall or proxy ACL rules and identify all active outbound connections to third-party license/permitting SaaS endpoints. On Linux: `ss -tunap | grep ESTABLISHED > vendor_connections_$(date +%F).txt`. On Windows: `Get-NetTCPConnection -State Established | Where-Object {$_.RemoteAddress -notlike '10.*' -and $_.RemoteAddress -notlike '192.168.*'} | Export-Csv vendor_connections.csv`. Cross-reference against your vendor contract inventory. Block at the perimeter firewall any vendor API endpoint that cannot be immediately verified as unrelated to the TPWD licensing vendor ecosystem.

Evidence: Before suspending any integration or modifying firewall rules, capture: (1) full `netstat -ano` or `Get-NetTCPConnection` output showing active sessions from vendor service accounts; (2) current authentication tokens and session cookies for vendor API connections from your API gateway or reverse proxy logs (e.g., nginx `access.log` at `/var/log/nginx/access.log`, IIS logs at `%SystemRoot%\System32\LogFiles\W3SVC`); (3) DNS query logs showing recent resolution of vendor-hosted license system domains — these volatile records will be overwritten once you block the integration. Document all active vendor IP ranges before any ACL change.

Step 2: Detection — Review access logs for your citizen or customer data systems for anomalous third-party API calls, unusual bulk data exports, or credential activity associated with vendor service accounts. Monitor for indicators consistent with T1078 (Valid Accounts) — off-hours logins, service accounts accessing data outside normal scope. Apply NIST AU-6 (Audit Record Review, Analysis, and Reporting) cadence. No public IOCs have been released for this incident.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis

Controls: NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST AU-2 (Event Logging), NIST AU-12 (Audit Record Generation), CIS 8.2 (Collect Audit Logs)

Compensating: Query Windows Security Event Log for Event ID 4624 (Successful Logon) and 4648 (Logon with Explicit Credentials) filtering on vendor service account names during off-hours (e.g., 10 PM–6 AM local): `Get-WinEvent -LogName Security | Where-Object {$_.Id -eq 4624 -and $_.Message -match 'vendor_svc_account'}`. For API gateway logs, run: `grep -E '(POST|GET).*/api/license|/api/citizen' /var/log/nginx/access.log | awk '{print $1, $7, $9}' | sort | uniq -c | sort -rn | head -50` to surface bulk query patterns. Deploy the free Sigma rule `win_susp_service_account_interactive_logon.yml` (available from SigmaHQ) to flag interactive logons by non-interactive service accounts.

Evidence: This is a detection/analysis step that does not alter live state, but preserve before any subsequent containment action: (1) raw API gateway or web server access logs showing vendor service account request volume and data query scope — pay particular attention to requests returning large row counts from citizen PII tables (hunting/fishing license holder name, DOB, address, license number); (2) Windows Security Event Log Event ID 4672 (Special Privileges Assigned) for vendor service accounts; (3) database query logs (SQL Server Profiler trace or PostgreSQL `pg_audit` log) showing SELECT statements against citizen data tables executed by vendor credentials; (4) authentication system logs showing the full session timeline for vendor service accounts in the 90 days prior to disclosure (March 4, 2026 baseline).

Step 3: Eradication — No patch is available; the attack vector targeted a vendor, not TPWD systems directly. Require the vendor to provide a written incident report, root cause analysis, and remediation plan. Rotate any shared credentials or API keys between your systems and affected or similarly positioned vendors. Apply D3-CRO (Credential Rotation) for all vendor-linked service accounts. Reference CIS 5.3 (Disable Dormant Accounts) and CIS 6.2 (Establish an Access Revoking Process) to remove stale vendor access.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST AC-2 (Account Management), CIS 5.3 (Disable Dormant Accounts), CIS 6.2 (Establish an Access Revoking Process), CIS 5.1 (Establish and Maintain an Inventory of Accounts)

Compensating: Enumerate all vendor-linked service accounts: `net user /domain | findstr /i 'vendor svc api'` or query your IdP directly. For each account: disable immediately in AD with `Disable-ADAccount -Identity `, then invalidate API keys by regenerating secrets in your API management layer (e.g., rotate keys in AWS API Gateway console or via `aws apigateway create-api-key`). Document each rotation with timestamp and responsible party in a shared incident log (even a timestamped Google Sheet works for a 2-person team). Cross-reference your account inventory against last-login timestamps to identify dormant vendor accounts inactive for 45+ days per CIS 5.3.

Evidence: CRITICAL — before rotating any credential or disabling any account, capture: (1) a full export of active sessions tied to vendor service accounts from your identity provider or LDAP (`Get-ADUser -Filter {Enabled -eq $true} -Properties LastLogonDate | Where-Object {$_.Name -match 'vendor'}`); (2) current API key usage logs from your API gateway showing the last request timestamp, source IP, and data payload size for each vendor credential — this establishes the access window for breach scope assessment; (3) a memory snapshot or running process list from any host where vendor agent software is installed, taken before the credential is revoked, as the agent may hold in-memory tokens or cached PII. These artifacts are destroyed the moment you rotate credentials.

Step 4: Recovery — Validate that vendor access to your environment is re-authorized only after documented remediation. Confirm audit logging is intact and has not been tampered with per NIST AU-9 (Protection of Audit Information). Re-enable vendor integrations under enhanced monitoring. Verify CIS 8.2 (Collect Audit Logs) is enforced for all vendor-touching systems. Notify affected individuals per applicable state breach notification law if your organization holds similar data.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST AU-9 (Protection of Audit Information), NIST AU-11 (Audit Record Retention), NIST AC-17 (Remote Access), CIS 8.2 (Collect Audit Logs), CIS 6.1 (Establish an Access Granting Process)

Compensating: Before re-enabling any vendor integration, verify log integrity: compare current log file sizes and last-modified timestamps against your pre-incident baseline (`ls -la --time-style=full-iso /var/log/app/ > post_incident_log_inventory.txt`). Check for log gaps by querying your syslog collector for the vendor-facing system's hostname — a gap during the suspected breach window indicates possible log tampering or deletion. Re-enable the integration behind a dedicated firewall rule with logging set to verbose, and use `tcpdump -i eth0 host -w vendor_reauth_$(date +%F).pcap` to capture the first 72 hours of re-established traffic for anomaly review.

Evidence: This step alters live state (re-enabling integrations and triggering new access). Before re-authorization, preserve: (1) a cryptographic hash (SHA-256) of all audit log files covering the breach window — `sha256sum /var/log/app/*.log > log_integrity_baseline.sha256` — to defend against future tampering claims; (2) a snapshot of the citizen data tables (row count, schema checksum) to establish a post-eradication integrity baseline for detecting any residual unauthorized modification to hunting/fishing license holder PII; (3) the vendor's written remediation attestation document, retained as a forensic record supporting potential Texas breach notification obligations under Texas Business and Commerce Code §521.

Step 5: Post-Incident — Conduct a full third-party risk assessment against all vendors with access to personal data. Establish or update vendor contracts to require breach notification timelines, security attestations, and right-to-audit clauses. Map vendor access to NIST AC-6 (Least Privilege) and AC-5 (Separation of Duties). Implement D3-UAP (User Account Permissions) reviews for all vendor service accounts. Develop or update a third-party incident response playbook aligned to NIST IR controls.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity

Controls: NIST AC-6 (Least Privilege), NIST AC-5 (Separation of Duties), NIST AU-6 (Audit Record Review, Analysis, and Reporting), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 6.1 (Establish an Access Granting Process), CIS 3.2 (Establish and Maintain a Data Inventory)

Compensating: Build a vendor access matrix in a spreadsheet: columns = vendor name, data classes accessed (PII, license data, payment data), access method (API key, VPN, RDP), last security attestation date, contract breach notification clause (Y/N). Prioritize vendors touching citizen PII identically to the TPWD pattern — name, DOB, address, license/permit number. Use osquery to periodically audit vendor service account permissions: `SELECT * FROM user_groups WHERE username LIKE '%vendor%';`. Draft a one-page third-party IR playbook checklist modeled on this incident's timeline: vendor notifies → internal triage within 4 hours → containment decision within 24 hours → breach notification assessment within 72 hours.

Evidence: No volatile evidence capture is required at this phase — this step does not alter live system state. Retain as permanent post-incident record: (1) the complete incident timeline document covering vendor notification date, internal discovery date, containment actions, and remediation verification — this is the evidentiary foundation for any Texas OAG inquiry; (2) the final scope assessment documenting how many citizen records (hunting/fishing license holders) were potentially exposed from your environment, mapped to data fields (name, DOB, address, license number, payment card data if applicable); (3) lessons-learned meeting notes identifying the specific control gap — absence of contractual breach notification SLA with the licensing vendor — that delayed detection, to anchor the playbook update.

Detection Guidance

No public IOCs have been released for this incident. Detection focus should shift to your own environment's third-party vendor access patterns. Query identity and access logs for service accounts associated with third-party vendors accessing citizen or customer data repositories. Flag bulk data exports, off-hours API calls, and access from unexpected source IPs tied to vendor accounts. Apply NIST AU-6 (Audit Record Review) cadence to audit records for vendor-facing integrations. For organizations using similar state-licensed system vendors, cross-reference vendor service account activity against known baselines. NIST AU-6 (Audit Record

Review) and NIST SI-7 (Software, Firmware, and Information Integrity) are applicable if vendor access touches local system resources. No specific event IDs or log signatures have been published as of available sources.

Framework Mappings

MITRE-ATTACK

- **T1078** — Valid Accounts
- **T1199** — Trusted Relationship

NIST-800-53R5

- **AC-2** — Account Management
- **AC-6** — Least Privilege
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **SR-2** — Supply Chain Risk Management Plan

HIPAA-SECURITY

- **164.308(a)(6)(ii)** — Response and Reporting

SOC2-TSC

- **CC7.4** — Responds to identified security incidents
- **CC9.2** — Manages risks associated with vendors and business partners

ISO-27001-2022

- **A.5.34** — Privacy and protection of personal information
- **A.5.21** — Managing information security in the ICT supply chain

NIST-CSF-2

- **RS.CO-03** — Recovery activities and progress communicated
- **GV.SC-01** — Cybersecurity supply chain risk management program

CIS-V8

- **15.1** — Establish and Maintain an Inventory of Service Providers

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1078	Valid Accounts	Defense-Evasion
T1199	Trusted Relationship	Initial-Access

Sources

Source	URL	Tier
Notification of Data Security Incident	https://tpwd.texas.gov/about/notification-of-data-security-incident	T1
A cybersecurity breach involving a vendor used by the Texas Parks ...	https://www.facebook.com/lonestaroutdoorshow/posts/yikessan-angelo-...	T3
Data breach exposes personal information of over 3 million Texas ...	https://www.kxan.com/news/texas/data-breach-hunting-fishing-licenses/	T3
What lessons can the Texas Parks & Wildlife Department learn from ...	https://www.quora.com/What-lessons-can-the-Texas-Parks-Wildlife-Dep...	T3
The Texas Parks and Wildlife Department says a cyberattack on its ...	https://www.instagram.com/p/DZ01TCwpBz-/	T3

Generated 2026-06-22 19:03 UTC by TJS Security Command Center