INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-04-14 18:30 UTC

ShinyHunters Exploits Salesforce Misconfiguration in McGraw-Hill Extortion Campaign, Platform-Wide Risk Suspected

DATA BREACH | HIGH | CVSS 7.5

SCC Item ID	SCC-DBR-2026-0092
Type	Data Breach
Severity	HIGH
CVSS Base Score	7.5
Affected Products	Salesforce (platform misconfiguration, specific version/product not disclosed); McGraw-Hill (confirmed victim); additional organizations suspected
Published	2026-04-14T14:07:07
Discovery Source	Rss

Executive Summary

ShinyHunters has breached McGraw-Hill via a Salesforce environment misconfiguration, claiming possession of 45 million PII records (unverified; McGraw-Hill disputes scale) and threatening public release by reported deadline of April 14. Salesforce has publicly acknowledged an active data extortion campaign tied to environment misconfigurations, suggesting the exposure extends beyond McGraw-Hill to other Salesforce tenants. The business risk is elevated: organizations using Salesforce for customer data management face potential regulatory exposure, reputational damage, and extortion pressure if their environments share the same misconfiguration class.

Technical Analysis

McGraw-Hill confirmed unauthorized access to data hosted on a Salesforce-managed webpage, with root cause attributed to a Salesforce environment misconfiguration rather than a software vulnerability. No CVE has been assigned. Relevant CWE mappings: CWE-732 (Incorrect Permission Assignment for Critical Resource), CWE-200 (Exposure of Sensitive Information to an Unauthorized Actor), CWE-284 (Improper Access Control). MITRE ATT&CK techniques observed or inferred: T1213 (Data from Information Repositories), T1530 (Data from Cloud Storage), T1078 (Valid Accounts), T1190 (Exploit Public-Facing Application), T1657 (Financial Threats), T1537 (Transfer Data to Cloud Account). ShinyHunters claims 45 million PII-containing records sourced from Salesforce infrastructure; McGraw-Hill disputes the scale. Confidence on record count: low, sourced from threat actor assertion, unverified by McGraw-Hill or Salesforce. Salesforce has issued a public

advisory at status.salesforce.com/generalmessages/20000244 acknowledging the extortion campaign. The misconfiguration class is suspected to affect multiple Salesforce tenants. No patch is applicable; remediation is configuration-based. CVSS base score of 7.5 assigned editorially based on impact severity; no NVD score available as this is a misconfiguration issue, not a software vulnerability.

Action Checklist

1. Step 1: Containment. Review all Salesforce org sharing settings, guest user permissions, and public-facing site configurations immediately. Disable guest user access on any Salesforce Experience Cloud or managed webpage that does not require it. Reference Salesforce advisory at status.salesforce.com/generalmessages/20000244 for specific misconfiguration classes flagged. (Note: Verify this URL resolves to current advisory before implementation.)
2. Step 2: Detection. Query Salesforce event logs (Setup Audit Trail, Event Monitoring if licensed) for anomalous data exports, guest user activity, bulk SOQL queries against Contact/Lead/Account objects, and API calls from unexpected IP ranges. Look for T1530 indicators: large-volume downloads from Salesforce-connected cloud storage. Check for T1078 indicators: dormant or low-privilege accounts with unexpected recent activity.
3. Step 3: Eradication. Correct identified misconfigurations: enforce field-level security, tighten object permissions, disable unnecessary public sharing rules, and remove any overly permissive guest user profiles. Review all connected third-party integrations for excessive OAuth scopes. Apply principle of least privilege across all Salesforce profiles and permission sets.
4. Step 4: Recovery. After remediation, run a Salesforce Health Check and Security Score audit within your org. Validate that no data export jobs or scheduled reports remain configured for external delivery. Monitor Event Monitoring logs for 30 days post-remediation for residual unauthorized access patterns. Confirm with Salesforce support that your org is not in scope for the current advisory.
5. Step 5: Post-Incident. This event exposes a systemic control gap: Salesforce misconfiguration risk is not consistently included in cloud security posture management (CSPM) programs. Map CWE-732 and CWE-284 gaps to your NIST CSF PR.AC and PR.DS controls. Add Salesforce org configuration to your recurring security review cadence. Evaluate whether Salesforce Event Monitoring (additional license) is warranted given data sensitivity.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate to legal, privacy counsel, and executive leadership immediately if Salesforce Login History or Event Monitoring logs confirm any guest user or API account accessed Contact, Lead, or Account objects containing PII (name, email, phone, SSN, DOB) in bulk — this triggers breach notification assessment obligations under GDPR (72-hour), CCPA, and applicable state laws given the 45M record scale claimed by ShinyHunters and the active extortion deadline of April 14.

Recovery Notes	Before restoring normal Salesforce operations, obtain written confirmation from Salesforce Support that your org ID is not flagged under advisory generalmessages/20000244 and re-run Salesforce Health Check to verify a materially improved Security Score against the pre-remediation baseline. Monitor Salesforce Login History and Setup Audit Trail weekly for 30 days post-remediation, specifically watching for any recurrence of guest user logins, API calls from previously unseen IP ranges, or bulk report execution against Contact/Lead/Account objects — patterns ShinyHunters used in the McGraw-Hill campaign. If Event Monitoring is not licensed, the 30-day manual monitoring cadence is non-negotiable given the active extortion campaign and the threat actor's stated April 14 public release deadline.
Forensic Artifacts	Salesforce Setup Audit Trail (CSV export, 180-day window): primary artifact for reconstructing ShinyHunters' configuration manipulation timeline — filter specifically for changes to Guest User profiles, Experience Cloud site sharing settings, Org-Wide Defaults on Contact/Lead/Account, and Permission Set assignments; this is the closest equivalent to a Windows Security Event Log for Salesforce administrative actions | Salesforce Login History (CSV export, 6-month window): reveals the IP addresses, user agents, and login types (API, UI, OAuth) used during the breach; bulk API logins from non-corporate IP ranges against guest or integration user accounts are the primary T1078 (Valid Accounts) indicator for this ShinyHunters campaign | Salesforce Event Monitoring logs — ReportEvent and ApiEvent types (if licensed): ReportEvent with RowsProcessed values exceeding 10,000 against Contact/Lead/Account objects is the forensic signature of ShinyHunters' bulk PII harvest (T1530); ApiEvent logs reveal the specific SOQL queries executed, object types queried, and data volumes returned per API session | Network perimeter proxy or firewall logs for outbound HTTPS connections to *.salesforce.com and *.force.com: unusually large response body sizes (multi-MB to GB range) in a compressed timeframe from a single source IP or user session indicate bulk data exfiltration; correlate source IPs against Salesforce Login History to confirm the exfiltration path used by ShinyHunters | Salesforce Connected Apps OAuth Usage report (Setup > Connected Apps OAuth Usage): identifies any third-party application granted broad OAuth scopes (full, api, read on Contact/Lead/Account) that may have been the initial access vector or pivot point; cross-reference grant timestamps against the ShinyHunters campaign timeline and Salesforce advisory disclosure date to identify potentially compromised integrations

Per-Action IR Details

Step 1: Containment — Review all Salesforce org sharing settings, guest user permissions, and public-facing site configurations immediately. Disable guest user access on any Salesforce Experience Cloud or managed webpage that does not require it. Reference Salesforce advisory at status.salesforce.com/generalmessages/20000244 for specific misconfiguration classes flagged.

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 — Containment Strategy: isolate affected components to prevent further data exposure without destroying forensic evidence; coordinate with platform owner (Salesforce) per active advisory.

Controls: NIST IR-4 (Incident Handling) — execute containment as part of the documented incident handling capability, NIST AC-2 (Account Management) — disable guest user accounts that are unnecessary or overly permissive in Salesforce Experience Cloud, NIST AC-17 (Remote Access) — restrict public-facing Salesforce site access to authorized sessions only, CIS 4.4 (Implement and Manage a Firewall on Servers) — enforce access restrictions at the Salesforce org boundary for public-facing Experience Cloud sites, CIS 6.2 (Establish an Access Revoking Process) — immediately revoke guest user access not required for business operations

Compensating: Without a CSPM tool, use Salesforce's built-in Security Health Check (Setup > Security Health Check) — it is free and flags guest user access, public sharing rules, and Experience Cloud exposure gaps. Run it

immediately and export the PDF report as a timestamped baseline. For orgs without Event Monitoring licenses, enable and download Setup Audit Trail (Setup > Setup Audit Trail > Download) going back 180 days before making any configuration changes, to preserve pre-containment state. Document every sharing rule and guest profile using the free Salesforce Optimizer report (Setup > Optimizer).

Evidence: BEFORE disabling guest users or changing sharing settings, capture: (1) Salesforce Setup Audit Trail export (CSV, 180-day window) showing all configuration changes — specifically filter for changes to Guest User profiles, Sharing Settings, Experience Cloud site configurations, and Permission Sets made in the 90 days prior to detection; (2) full export of current Guest User profile permissions and assigned permission sets via Setup > Profiles > Guest User Profile; (3) Salesforce Org-Wide Default (OWD) sharing settings snapshot for Contact, Lead, Account, and any custom objects containing PII; (4) list of all active public sites under Setup > Sites and Digital Experiences, including associated guest user license counts.

Step 2: Detection — Query Salesforce event logs (Setup Audit Trail, Event Monitoring if licensed) for anomalous data exports, guest user activity, bulk SOQL queries against Contact/Lead/Account objects, and API calls from unexpected IP ranges. Look for T1530 indicators: large-volume downloads from Salesforce-connected cloud storage. Check for T1078 indicators: dormant or low-privilege accounts with unexpected recent activity.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis: correlate event log data across Salesforce audit sources to reconstruct ShinyHunters' access timeline, identify exfiltrated object types, and establish scope of the 45M record claim.

Controls: NIST AU-2 (Event Logging) — ensure Salesforce login history, API usage, and report execution events are captured for analysis, NIST AU-6 (Audit Record Review, Analysis, and Reporting) — conduct focused review of Salesforce event logs for bulk data access patterns consistent with ShinyHunters' exfiltration methodology, NIST SI-4 (System Monitoring) — monitor for MITRE ATT&CK T1530 (Data from Cloud Storage) indicators in Salesforce-connected storage and T1078 (Valid Accounts) dormant account activity, NIST IR-5 (Incident Monitoring) — track and document all detected anomalous events in Salesforce logs as part of ongoing incident tracking, CIS 8.2 (Collect Audit Logs) — confirm Salesforce login history, report runs, and API call logs are being collected and retained

Compensating: Without Event Monitoring license, use these free Salesforce native queries in the Developer Console (Setup > Developer Console > Query Editor): (1) Bulk SOQL against Contact/Lead: SELECT Id, Name, LoginTime, SourceIp, UserId FROM LoginHistory WHERE LoginTime = LAST_N_DAYS:90 ORDER BY LoginTime DESC; (2) Report execution: SELECT Id, Name, LastRunDate, LastModifiedById FROM Report WHERE LastRunDate = LAST_N_DAYS:90 ORDER BY LastRunDate DESC — flag reports on Contact, Lead, or Account objects run by guest or API-only users; (3) Data export jobs: Setup > Data Export — check for scheduled or recent manual exports. For T1078 dormant account analysis, run: SELECT Id, Name, LastLoginDate, IsActive, Profile.Name FROM User WHERE LastLoginDate < LAST_N_DAYS:90 AND IsActive = true ORDER BY LastLoginDate ASC. Export all results to CSV and preserve with MD5 hash before proceeding.

Evidence: Capture BEFORE any eradication: (1) Salesforce Login History for all users (Setup > Login History, export full 6-month range) — filter on guest user logins and API logins from IPs outside your known corporate ranges, specifically looking for high-volume sessions characteristic of automated SOQL scraping; (2) Salesforce Report Run History if Event Monitoring is licensed — EventType = ReportEvent, filter for records with RowsProcessed > 10000 against Contact/Lead/Account objects; (3) Connected App OAuth token grants (Setup > Connected Apps OAuth Usage) — identify any third-party app with access to Contact/Lead/Account read scopes that was granted access within the past 180 days; (4) Salesforce API usage logs from your network perimeter firewall or proxy showing outbound HTTPS traffic to *.salesforce.com or *.force.com with unusually large response body sizes, correlating to T1530 bulk download patterns; (5) For T1078: User login records for any account with LastLoginDate older than 90 days that shows activity in the past 30 days, particularly accounts assigned to integrations or with API-only profiles.

Step 3: Eradication — Correct identified misconfigurations: enforce field-level security, tighten object permissions, disable unnecessary public sharing rules, and remove any overly permissive guest user profiles. Review all connected third-party integrations for excessive OAuth scopes. Apply principle of least privilege across all Salesforce profiles and permission sets.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication: remove the misconfiguration root cause that enabled ShinyHunters' access; verify all overly permissive sharing rules and guest profiles are eliminated before declaring the environment clean.

Controls: NIST SI-2 (Flaw Remediation) — remediate the Salesforce misconfiguration classes identified in the Salesforce advisory (status.salesforce.com/generalmessages/20000244) as security flaws requiring correction, NIST AC-6 (Least Privilege) — enforce least privilege across all Salesforce profiles, permission sets, and connected app OAuth scopes, NIST AC-3 (Access Enforcement) — correct object-level and field-level security on Contact, Lead, and Account objects to prevent unauthorized read access, NIST CM-7 (Least Functionality) — disable unnecessary public sharing rules and guest user capabilities that expose PII objects, CIS 3.3 (Configure Data Access Control Lists) — reconfigure Salesforce object and field permissions so Contact/Lead/Account PII is accessible only on a need-to-know basis, CIS 4.7 (Manage Default Accounts on Enterprise Assets and Software) — remove or lock default guest user profiles in Salesforce Experience Cloud that ship with overly broad permissions

Compensating: Without a dedicated Salesforce security tool, use the free Salesforce Permission Analyzer (available in AppExchange at no cost for basic tier) to enumerate effective permissions per profile before and after changes. For field-level security review, use the Salesforce CLI (sf) with the command: sf org display --target-org and pull permission set assignments via: sf data query --query "SELECT Id, PermissionsViewAllData, PermissionsModifyAllData, Profile.Name FROM PermissionSet WHERE IsOwnedByProfile = false" — flag any permission set with ViewAllData or ModifyAllData. For OAuth scope review, revoke and re-authorize any connected app with scope=full or scope=api where scope=read-specific-objects would suffice. Document each change with a before/after screenshot and store in your incident ticket.

Evidence: Before executing eradication changes: (1) export full current sharing rule configuration (Setup > Sharing Settings) as a PDF or screenshot — specifically capture Org-Wide Defaults for Contact, Lead, Account, and any custom objects containing email, phone, or SSN fields; (2) export all Guest User profile permissions including object permissions, field permissions, and assigned permission sets — this establishes the misconfigured baseline that enabled the breach; (3) export Connected Apps list with OAuth scopes (Setup > Connected Apps > Manage Connected Apps) — document scope grants for any app with access to Contact/Lead/Account; (4) capture Salesforce Health Check score before remediation (Setup > Security Health Check > Export) to document the pre-remediation risk posture for regulatory and legal record.

Step 4: Recovery — After remediation, run a Salesforce Health Check and Security Score audit within your org. Validate that no data export jobs or scheduled reports remain configured for external delivery. Monitor Event Monitoring logs for 30 days post-remediation for residual unauthorized access patterns. Confirm with Salesforce support that your org is not in scope for the current advisory.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery: restore the Salesforce environment to a verified-secure state, confirm residual access paths are closed, and establish a 30-day enhanced monitoring window consistent with the advisory's active exploitation context.

Controls: NIST IR-4 (Incident Handling) — execute recovery phase activities including verification that eradication was successful and monitoring for recurrence, NIST SI-6 (Security and Privacy Function Verification) — verify that corrected Salesforce sharing settings, guest user controls, and field-level security are functioning as intended post-remediation, NIST AU-6 (Audit Record Review, Analysis, and Reporting) — conduct enhanced review of Salesforce event logs for 30 days post-remediation to detect any residual unauthorized access, NIST CP-10 (System Recovery and Reconstitution) — confirm Salesforce org is restored to a known-secure configuration baseline before resuming normal operations, CIS 7.1 (Establish and Maintain a Vulnerability Management Process) — validate that Salesforce Health Check and Security Score confirm remediation effectiveness before closing the incident

Compensating: Without Event Monitoring license for the 30-day watch period, configure free Salesforce native alerting: (1) Setup > Security > Session Settings — enable and log all session security changes; (2) create a Salesforce Flow or Process Builder alert that triggers on bulk Report runs against Contact/Lead objects (threshold: >1000 records) and sends email notification to the security team; (3) schedule a weekly manual pull of Login History CSV (Setup > Login History > Download) filtered on guest user and API profile logins — compare week-over-week for new IP ranges; (4) set a calendar reminder to re-run Salesforce Health Check weekly for the 30-day window and

compare scores against the post-remediation baseline export.

Evidence: Before declaring recovery complete: (1) Salesforce Health Check post-remediation export (PDF) showing improved score — retain alongside the pre-remediation baseline for regulatory documentation; (2) Data Export job list (Setup > Data Management > Data Export) — confirm no scheduled exports remain active or were created by the attacker during the breach window; (3) Scheduled Reports list (Reports tab > All Scheduled Reports) — confirm no reports are configured for external email delivery to non-corporate addresses; (4) Salesforce Optimizer post-remediation run — retain as evidence that configuration improvements were implemented; (5) written confirmation from Salesforce Support (case number retained) that your specific org ID is not flagged under the active advisory scope.

Step 5: Post-Incident — This event exposes a systemic control gap: Salesforce misconfiguration risk is not consistently included in cloud security posture management (CSPM) programs. Map CWE-732 and CWE-284 gaps to your NIST CSF PR.AC and PR.DS controls. Add Salesforce org configuration to your recurring security review cadence. Evaluate whether Salesforce Event Monitoring (additional license) is warranted given data sensitivity.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity: conduct lessons-learned review to identify the systemic control gap that allowed ShinyHunters to exploit Salesforce misconfiguration; update policies, detection capabilities, and review cadence to prevent recurrence across all Salesforce tenants.

Controls: NIST IR-4 (Incident Handling) — incorporate Salesforce misconfiguration scenarios into the documented incident handling capability, NIST IR-8 (Incident Response Plan) — update the IR plan to include SaaS platform misconfiguration as a named incident category with Salesforce-specific detection and containment procedures, NIST SI-2 (Flaw Remediation) — establish a recurring Salesforce configuration review process that treats misconfiguration classes from CWE-732 (Incorrect Permission Assignment) and CWE-284 (Improper Access Control) as remediable flaws, NIST RA-3 (Risk Assessment) — update organizational risk assessment to include Salesforce SaaS misconfiguration as a distinct risk scenario tied to the 45M PII record exposure potential demonstrated in this campaign, NIST AU-2 (Event Logging) — evaluate Salesforce Event Monitoring license acquisition as a compensating control given the data sensitivity of Contact/Lead/Account objects, CIS 7.1 (Establish and Maintain a Vulnerability Management Process) — extend vulnerability management process to include SaaS configuration drift for Salesforce, treating Health Check score degradation as a vulnerability finding, CIS 7.2 (Establish and Maintain a Remediation Process) — add Salesforce misconfiguration findings to the risk-based remediation process with defined SLAs for Critical/High Health Check findings, CIS 8.2 (Collect Audit Logs) — formally include Salesforce Setup Audit Trail and (where licensed) Event Monitoring in the enterprise audit log collection program

Compensating: Without budget for Salesforce Event Monitoring or a CSPM tool, implement a free recurring review using: (1) Salesforce Health Check — schedule a quarterly export and track score trends in a shared spreadsheet; assign ownership to a named team member; (2) free Salesforce Security Center (available to orgs with multiple Salesforce products) for cross-org visibility; (3) publish a Sigma rule for your SIEM (if available) that alerts on new Salesforce OAuth app grants from your identity provider logs — Sigma community has Salesforce-specific detection rules at github.com/SigmaHQ/sigma (search 'Salesforce'); (4) for CWE-732/CWE-284 mapping, use the free NIST NVD CWE browser to document findings in your GRC tracking tool with a Salesforce-specific control gap record; (5) add Salesforce org configuration review as a standing agenda item in quarterly security reviews using the free Salesforce Optimizer report as the input artifact.

Evidence: Preserve for lessons-learned and potential regulatory response: (1) full incident timeline document mapping the first suspicious Salesforce event to detection, containment, eradication, and recovery — required for GDPR 72-hour notification assessment and state breach notification law triggers given PII scope; (2) pre- and post-remediation Salesforce Health Check exports showing the specific misconfiguration classes corrected — maps directly to CWE-732 and CWE-284 for regulatory disclosure; (3) list of Salesforce object types and estimated record counts accessible during the exposure window — required for breach notification scope determination under CCPA, GDPR, and applicable state laws; (4) Salesforce Support case record confirming advisory scope assessment for your org; (5) updated IR plan and Salesforce configuration review policy documents with effective dates, demonstrating that systemic control gaps were addressed post-incident.

Detection Guidance

Query Salesforce Event Monitoring logs (if licensed) for: bulk API queries against PII-bearing objects (Contact, Lead, Account, PersonAccount) exceeding normal volume thresholds; guest user logins followed by data access events; large file exports or report downloads to external destinations. In Setup Audit Trail, look for recent changes to sharing rules, guest user profiles, or public site configurations. If Event Monitoring is not licensed, review standard login history and data export service logs. Behavioral indicators include unexpected SOQL query volume spikes, API calls from IPs not associated with known integrations, and guest user sessions with data read events. No specific IOCs (IPs, domains, hashes) have been publicly confirmed for this campaign at the time of this writing.

Indicators of Compromise

Type	Value	Context	Confidence
DOMAIN	`ShinyHunters dark-web extortion portal`	ShinyHunters listed McGraw-Hill on a dark-web extortion portal with an April 14 deadline. Specific URL not published in available sources to avoid amplification.	LOW

Framework Mappings

MITRE-ATTACK

- **T1213** — Data from Information Repositories
- **T1530** — Data from Cloud Storage
- **T1078** — Valid Accounts
- **T1190** — Exploit Public-Facing Application
- **T1657** — Financial Theft
- **T1537** — Transfer Data to Cloud Account

NIST-800-53R5

- **AC-2** — Account Management
- **AC-6** — Least Privilege
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **CA-8** — Penetration Testing
- **RA-5** — Vulnerability Monitoring and Scanning
- **SC-7** — Boundary Protection
- **SI-2** — Flaw Remediation
- **SI-7** — Software, Firmware, and Information Integrity
- **AC-3** — Access Enforcement

- **SC-28** — Protection of Information at Rest

OWASP-TOP10-2021

- **A01:2021** — Broken Access Control

HIPAA-SECURITY

- **164.312(a)(1)** — Access Control

CIS-V8

- **6.1** — Establish an Access Granting Process
- **6.2** — Establish an Access Revoking Process
- **3.3** — Configure Data Access Control Lists

SOC2-TSC

- **CC6.1** — The entity implements logical access security software, infrastructure, and architectures over protected information assets
- **CC6.3** — Authorizes, modifies, or removes access

ISO-27001-2022

- **A.8.8** — Management of technical vulnerabilities
- **A.5.34** — Privacy and protection of personal information

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1213	Data from Information Repositories	Collection
T1530	Data from Cloud Storage	Collection
T1078	Valid Accounts	Defense-Evasion
T1190	Exploit Public-Facing Application	Initial-Access
T1657	Financial Theft	Impact
T1537	Transfer Data to Cloud Account	Exfiltration

Sources

Source	URL	Tier
Security News	https://www.bleepingcomputer.com/news/security/mcgraw-hill-confirms...	T3
McGraw-Hill confirms data breach following extortion threat	https://www.instagram.com/p/DXHyHYojwFi/	T3

Source	URL	Tier
The Salesforce Misconfiguration Leading to Massive Data Breaches	https://www.youtube.com/watch?v=6Z2Z8c9HEEA	T3
20000244 - Salesforce Status	https://status.salesforce.com/generalmessages/20000244	T3
Salesforce Sounds Alarm Over Fresh Data Extortion Campaign	https://www.govinfosecurity.com/salesforce-sounds-alarm-over-fresh-...	T3

Generated 2026-04-14 18:30 UTC by TJS Security Command Center