INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-05-12 06:37 UTC

Instructure Canvas hack update: Breach involved a specific teacher account type and interrupted finals

DATA BREACH | HIGH | CVSS 7.5

SCC Item ID	SCC-DBR-2026-0122
Type	Data Breach
Severity	HIGH
CVSS Base Score	7.5
Affected Products	Instructure Canvas LMS (Learning Management System), Free-For-Teacher account tier
Published	15 hours ago
Discovery Source	Serper

Executive Summary

ShinyHunters, a financially motivated threat group with a history of large-scale data theft, breached Instructure's Canvas learning management platform by compromising the 'Free-For-Teacher' account tier. The incident caused platform downtime that disrupted student access during finals periods and exposed student and educator data to potential exfiltration, extortion, or sale. Organizations and institutions using Canvas should audit third-party and free-tier account access and assess what data may have been reachable from compromised accounts.

Technical Analysis

The breach affected Instructure Canvas LMS, specifically through compromise of the 'Free-For-Teacher' account tier, a lower-security account class distinct from institutional single-sign-on accounts. The precise attack vector has not been publicly confirmed; candidate mechanisms include credential stuffing (T1078), cloud account takeover (T1078.004), or API-level data access (T1530). Post-access, ShinyHunters' operational pattern aligns with financial extortion or data sale (T1657). No CVE has been assigned; the breach is an access control failure rather than a software vulnerability. Applicable CWEs are CWE-284 (Improper Access Control) and CWE-287 (Improper Authentication). No vendor-issued patch exists for a software flaw; remediation centers on credential hygiene, access tier controls, and account segmentation. Canvas service has been restored. Sources cited are Tier 3 (Mashable, PCMag, Yahoo Tech, Reddit, WRAL); no Tier 1 or Tier 2 source has been included in this report as of the configuration date.

Action Checklist

1. Containment: Audit all Free-For-Teacher and non-institutional Canvas accounts associated with your organization. Suspend or disable accounts not provisioned through your institutional identity provider. Revoke active sessions for accounts in that tier via Canvas admin controls.
2. Detection: Review Canvas admin audit logs for anomalous access patterns from Free-For-Teacher accounts: off-hours logins, bulk data exports, API calls to course roster or gradebook endpoints, or access from unexpected geolocations. Check identity provider logs for authentication events that bypassed SSO.
3. Eradication: Enforce institutional SSO as the sole authentication path for all users accessing organizational Canvas environments. Disable or restrict Free-For-Teacher account creation and access within your tenant where policy permits. Rotate credentials for any shared or service accounts with Canvas API access.
4. Recovery: Confirm all active sessions for affected account tiers have been terminated. Validate that SSO enforcement is active and that no Free-For-Teacher accounts retain elevated data access. Monitor Canvas API access logs for 30 days post-remediation for residual anomalous activity.
5. Post-Incident: Evaluate whether your institution's data classification policy covers LMS-resident data (grades, PII, course materials). Assess whether Free-For-Teacher or similar low-assurance account tiers represent a standing gap in your identity governance program. Update third-party and free-tier account provisioning policies accordingly.

IR / Forensic Enrichment

Triage Priority	URGENT
Escalation Criteria	Escalate immediately to institutional legal counsel and data privacy officer if Canvas audit logs confirm that ShinyHunters-associated accounts accessed or exported FERPA-protected student records (grades, enrollment data, PII), as this triggers mandatory breach notification obligations under FERPA and potentially state-level student privacy statutes; escalate to Instructure's incident response team via their Trust & Security portal if forensic evidence indicates the compromise extended beyond Free-For-Teacher accounts to institutional SSO-provisioned users.
Recovery Notes	Verify recovery by running a post-remediation authentication audit confirming all Canvas logins are sourced exclusively from your institutional SSO provider, with zero direct-credential or FFT-tier authentications present in the audit log. Monitor the Canvas API access logs and IdP authentication events daily for 30 days, specifically watching for re-enrollment of FFT-type accounts, API token usage from previously revoked service accounts, or authentication attempts from IP ranges associated with ShinyHunters infrastructure identified during the detection phase. Contact Instructure support to request confirmation of the platform-side remediation status and obtain their incident timeline to correlate against your tenant-level forensic evidence.

Forensic Artifacts	Canvas Admin Audit Log (JSON export via GET /api/v1/audit/authentication/accounts/:account_id): captures login timestamps, source IPs, authentication method (SAML vs. direct credential), and user_id for all FFT-tier accounts — primary artifact for establishing ShinyHunters actor timeline and confirming SSO bypass. | Canvas Grade Change Audit Log (GET /api/v1/audit/grade_change/courses/:course_id): records all gradebook read and write events by user_id and timestamp — use to determine whether FERPA-protected grade data was accessed or modified by FFT accounts during the incident window. | IdP Authentication Logs (Okta System Log, Azure AD Sign-In Logs, or Shibboleth IdP audit log): filter for Canvas SP entityID assertions to identify any authentication flows that completed without MFA challenge or that originated from anomalous geolocations consistent with ShinyHunters infrastructure. | Canvas API Developer Key and Token Access Logs (Admin > Developer Keys): enumerate all API tokens generated by or assigned to FFT-tier accounts, capturing token creation dates, last-used timestamps, and associated scopes — critical for determining whether bulk data extraction occurred via API rather than UI. | Institutional network perimeter or reverse-proxy logs (nginx access.log or equivalent) for the Canvas application tier: filter for high-frequency requests to /api/v1/courses/:id/enrollments, /api/v1/courses/:id/students, and /api/v1/courses/:id/gradebook_history from a single source IP within short time windows — characteristic pattern of ShinyHunters-style bulk data staging prior to exfiltration.

Per-Action IR Details

Containment — Audit all Free-For-Teacher and non-institutional Canvas accounts associated with your organization. Suspend or disable accounts not provisioned through your institutional identity provider. Revoke active sessions for accounts in that tier via Canvas admin controls.

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 — Containment Strategy: isolate affected account tier to prevent continued unauthorized access to course rosters, gradebooks, and student PII within the Canvas tenant.

Controls: NIST IR-4 (Incident Handling), NIST AC-2 (Account Management), CIS 5.3 (Disable Dormant Accounts), CIS 6.2 (Establish an Access Revoking Process)

Compensating: Export the Canvas Admin Console user list via Settings > Users > Export CSV, then filter for account type 'Free-For-Teacher' using: grep -i 'free_for_teacher' canvas_users_export.csv > fft_accounts.csv. Cross-reference against your IdP's provisioned user list using a Python one-liner (set diff) to identify orphaned accounts. Use the Canvas Admin API endpoint GET /api/v1/accounts/:account_id/users with the 'enrollment_type' parameter to enumerate non-SSO users if CSV export is incomplete. Session termination can be forced per user via the Canvas Admin UI under People > [User] > Reset Session.

Evidence: Before suspending accounts, capture the full Canvas Admin user export (CSV) showing account type, last login timestamp, login IP, and authentication method for all Free-For-Teacher accounts. Pull Canvas Admin Audit Log entries (Admin Console > Audit Log) filtered to the FFT account tier for the 90 days prior to the incident, preserving records of any course enrollment actions, gradebook access, or file download events initiated by these accounts. Screenshot or export active session tokens from Canvas Admin > People to document which sessions were live at containment time.

Detection — Review Canvas admin audit logs for anomalous access patterns from Free-For-Teacher accounts: off-hours logins, bulk data exports, API calls to course roster or gradebook endpoints, or access from unexpected geolocations. Check identity provider logs for authentication events that bypassed SSO.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis: correlate Canvas audit log data with IdP authentication records to establish timeline of ShinyHunters actor activity and confirm whether exfiltration of student PII or gradebook data occurred.

Controls: NIST IR-5 (Incident Monitoring), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST AU-12 (Audit Record Generation), NIST SI-4 (System Monitoring), CIS 8.2 (Collect Audit Logs)

Compensating: Query Canvas Admin Audit Logs via the API: GET /api/v1/audit/authentication/accounts/:account_id — filter results for login_type != 'saml' or login_type != 'cas' to surface direct-credential authentications that bypassed SSO. For bulk data export detection, query the Canvas API event log endpoint GET /api/v1/audit/grade_change/courses/:course_id and look for high-frequency gradebook read events from a single FFT user_id within a short time window. Parse IdP logs (Okta, Azure AD, or Shibboleth) for auth events where the Canvas SP entityID appears without a corresponding MFA challenge. Use jq to filter JSON audit output: jq '.[] | select(.event_type == "login" and .pseudonym.unique_id | contains("@") | not)' audit_log.json to flag non-institutional email logins.

Evidence: Preserve Canvas Admin Audit Log exports (JSON and CSV) for the full retention window, specifically filtering for: (1) API calls to /api/v1/courses/:id/enrollments and /api/v1/courses/:id/gradebook_history from FFT account user_ids, (2) authentication events showing login via username/password rather than SAML/SSO, and (3) geolocation data on login IPs — cross-reference against threat intelligence for ShinyHunters-associated infrastructure. Capture IdP authentication logs showing Canvas SP assertions without MFA completion. Preserve web server or reverse-proxy access logs (nginx/Apache) for the Canvas application tier showing URI patterns matching /api/v1/ bulk data endpoints with high request rates from a single source IP.

Eradication — Enforce institutional SSO as the sole authentication path for all users accessing organizational Canvas environments. Disable or restrict Free-For-Teacher account creation and access within your tenant where policy permits. Rotate credentials for any shared or service accounts with Canvas API access.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication: remove the attack vector by eliminating the low-assurance Free-For-Teacher authentication path that ShinyHunters exploited to gain initial access to the Canvas tenant.

Controls: NIST IR-4 (Incident Handling), NIST IA-2 (Identification and Authentication — Organizational Users), NIST AC-17 (Remote Access), NIST SI-2 (Flaw Remediation), CIS 6.3 (Require MFA for Externally-Exposed Applications), CIS 6.5 (Require MFA for Administrative Access), CIS 4.7 (Manage Default Accounts on Enterprise Assets and Software)

Compensating: In Canvas Admin Settings, navigate to Authentication > Add New Provider and verify SAML or CAS is the only active authentication provider — remove or disable the Canvas built-in authentication provider if your tenant supports it. To restrict FFT account creation, submit a configuration request to Instructure support referencing your institutional contract, or enforce domain-based enrollment restrictions under Account Settings > Restrict enrollments to institution domains. For Canvas API service account token rotation: identify all active tokens via GET /api/v1/users/:user_id/tokens for each service account, delete existing tokens via DELETE /api/v1/users/:user_id/tokens/:id, and generate new tokens with expiration dates set — document token owners in a credentials register. Use a bash loop against the Canvas API to enumerate all active service account tokens across admin-level accounts before rotation.

Evidence: Before enforcing SSO-only authentication, capture the current Canvas Authentication Providers configuration (Admin > Settings > Authentication screenshot or API response from GET /api/v1/accounts/:id/authentication_providers) to document what authentication methods were active during the incident window. Export all Canvas API developer keys and service account tokens via Admin > Developer Keys to establish a pre-rotation baseline. Preserve any Canvas LTI integration configurations that may use service accounts, as these represent additional credential rotation scope.

Recovery — Confirm all active sessions for affected account tiers have been terminated. Validate that SSO enforcement is active and that no Free-For-Teacher accounts retain elevated data access. Monitor Canvas API access logs for 30 days post-remediation for residual anomalous activity.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery: verify that the Canvas environment has been restored to a known-good authentication state, with ongoing monitoring to detect any persistence mechanisms or re-entry attempts by the ShinyHunters actor.

Controls: NIST IR-4 (Incident Handling), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST SI-7 (Software, Firmware, and Information Integrity), NIST CA-7 (Continuous Monitoring), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: Validate session termination by querying GET /api/v1/accounts/:id/users filtered to FFT account type and confirming no active session tokens remain — cross-check against the pre-containment session export captured in Step 1. Verify SSO enforcement by attempting a test login with a known FFT-type credential from an out-of-band device; a correctly configured tenant should reject the authentication or redirect to IdP. For 30-day monitoring without SIEM, create a daily cron job that pulls Canvas API authentication audit logs via GET /api/v1/audit/authentication/accounts/:account_id, pipes through jq to filter for non-SAML login events, and emails the output to the security team: 0 6 * * * curl -H 'Authorization: Bearer TOKEN' 'https://canvas.instructure.com/api/v1/audit/authentication/accounts/ACCT_ID' | jq '.[] | select(.event_type=="login" and .pseudonym.authentication_provider_type != "saml")' | mail -s 'Canvas Non-SSO Login Report' security@yourorg.edu

Evidence: Before closing the recovery phase, capture a final Canvas Admin user export confirming zero active FFT accounts with course admin, TA, or instructor roles. Pull a post-remediation authentication audit log snapshot to establish a clean baseline for the 30-day monitoring window. Document the state of all Canvas course enrollments modified during the incident window by querying GET /api/v1/audit/course/courses/:course_id for each affected course, preserving records of any enrollment additions made by FFT accounts that may need reversal.

Post-Incident — Evaluate whether your institution's data classification policy covers LMS-resident data (grades, PII, course materials). Assess whether Free-For-Teacher or similar low-assurance account tiers represent a standing gap in your identity governance program. Update third-party and free-tier account provisioning policies accordingly.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity: conduct lessons-learned review to address the systemic identity governance gap that allowed a non-institutional account tier to access student PII, gradebook data, and course materials within the Canvas LMS.

Controls: NIST IR-8 (Incident Response Plan), NIST RA-2 (Security Categorization), NIST AU-11 (Audit Record Retention), NIST SI-5 (Security Alerts, Advisories, and Directives), CIS 5.1 (Establish and Maintain an Inventory of Accounts), CIS 6.1 (Establish an Access Granting Process), CIS 3.2 (Establish and Maintain a Data Inventory)

Compensating: Conduct a lessons-learned meeting within 2 weeks of incident closure using the NIST 800-61r3 §4 discussion template — document the specific finding that Instructure's FFT account tier bypassed institutional identity controls and resulted in access to FERPA-protected student records. Update the institution's data classification inventory (CIS 3.2) to explicitly tag Canvas-resident data types (FERPA-protected grades and enrollment records, PII, course IP) with their sensitivity tier. Draft a third-party and free-tier account provisioning policy that requires all accounts with access to LMS data to be provisioned through the institutional IdP — use this incident as the documented risk justification. Review Instructure's published advisory and any subsequent security bulletins via the Instructure Trust & Security portal to confirm no additional FFT-tier vulnerabilities have been disclosed.

Evidence: Compile the complete incident timeline from Canvas audit logs, IdP authentication records, and admin action logs to support the lessons-learned review and any required FERPA breach notification assessment. Preserve all forensic artifacts from earlier phases (audit log exports, session records, API access logs) per your institution's records retention policy — minimum 3 years for FERPA-related incidents. If student PII or grades were confirmed or suspected as accessed, document the data elements involved, the number of affected students, and the date of discovery to support institutional legal counsel's breach notification analysis.

Detection Guidance

No confirmed IOCs (IPs, domains, file hashes) have been publicly released for this incident as of current reporting. Detection should focus on behavioral indicators in Canvas admin and API logs: (1) authentication events from Free-For-Teacher accounts outside normal hours or from anomalous geographies; (2) bulk access to course rosters, gradebooks, or user directories via API; (3) large data export events initiated by

non-institutional accounts; (4) repeated failed authentication followed by successful login consistent with credential stuffing. Cross-reference Canvas access logs with your IdP logs to identify accounts that authenticated outside your SSO flow. ShinyHunters TTPs historically include rapid bulk exfiltration following initial access; prioritize data egress indicators in addition to access anomalies.

Framework Mappings

MITRE-ATTACK

- **T1078.004** — Cloud Accounts
- **T1657** — Financial Theft
- **T1078** — Valid Accounts
- **T1530** — Data from Cloud Storage

NIST-800-53R5

- **AC-2** — Account Management
- **AC-6** — Least Privilege
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **AC-3** — Access Enforcement
- **IA-8** — Identification and Authentication (Non-Organizational Users)

OWASP-TOP10-2021

- **A01:2021** — Broken Access Control
- **A07:2021** — Identification and Authentication Failures

CIS-V8

- **6.1** — Establish an Access Granting Process
- **6.2** — Establish an Access Revoking Process
- **6.3** — Require MFA for Externally-Exposed Applications
- **6.4** — Require MFA for Remote Network Access
- **6.5** — Require MFA for Administrative Access

SOC2-TSC

- **CC6.1** — The entity implements logical access security software, infrastructure, and architectures over protected information assets
- **CC7.4** — Responds to identified security incidents

HIPAA-SECURITY

- **164.312(a)(1)** — Access Control
- **164.312(d)** — Person or Entity Authentication
- **164.308(a)(6)(ii)** — Response and Reporting

ISO-27001-2022

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

NIST-CSF-2

- **RS.CO-03** — Recovery activities and progress communicated

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1078.004	Cloud Accounts	Defense-Evasion
T1657	Financial Theft	Impact
T1078	Valid Accounts	Defense-Evasion
T1530	Data from Cloud Storage	Collection

Sources

Source	URL	Tier
	https://mashable.com/article/instructure-canvas-hack-data-breach-sh...	T3
Instructure Canvas hack update: Breach involved a specific teacher ...	https://tech.yahoo.com/cybersecurity/articles/instructure-canvas-ha...	T3
Canvas Restored After Hack, Breach Traced to 'Free-For-Teacher ...	https://www.reddit.com/r/technology/comments/1t92yae/canvas_restore...	T3
Canvas data breach ■■ There has been a cybersecurity incident ...	https://www.facebook.com/WRALTV/posts/canvas-data-breach-%EF%B8%8F-...	T3
Canvas Restored After Hack, Breach Traced to 'Free-For-Teacher ...	https://www.pcmag.com/news/canvas-restored-after-hack-breach-traced...	T3

Generated 2026-05-12 06:37 UTC by TJS Security Command Center