INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-05-04 06:06 UTC

ShinyHunters Claims 275 Million Records from Instructure Canvas Breach, Education Sector Faces Largest LMS Compromise on Record

DATA BREACH | HIGH | CVSS 9.5

SCC Item ID	SCC-DBR-2026-0112
Type	Data Breach
Severity	HIGH
CVSS Base Score	9.5
Affected Products	Instructure Canvas LMS (multi-tenant SaaS platform); Salesforce (alleged secondary compromise, unconfirmed); approximately 15,000 institutions globally
Published	2026-05-03T18:16:27
Discovery Source	Rss

Executive Summary

Instructure, operator of the Canvas learning management system used by approximately 15,000 institutions globally, has confirmed a cybersecurity incident exposing student and institutional data including names, email addresses, student ID numbers, and private messages. Threat actor ShinyHunters claims to have exfiltrated 275 million records and has listed Instructure on its extortion site, though the record count is unverified and should be treated with caution. This is Instructure's second disclosed incident within eight months, indicating a potential unresolved systemic exposure across a platform that serves K-12, higher education, and corporate learning environments worldwide.

Technical Analysis

Instructure Canvas, a multi-tenant SaaS LMS, has confirmed unauthorized access resulting in data exfiltration. ShinyHunters claims 275 million records across approximately 15,000 institutions; Instructure's disclosure does not confirm this volume. Associated CWEs suggest credential-based initial access or API/integration layer exploitation: CWE-284 (Improper Access Control), CWE-522 (Insufficiently Protected Credentials), and CWE-200 (Exposure of Sensitive Information to an Unauthorized Actor). No CVE has been assigned. Relevant MITRE ATT&CK techniques include T1078 (Valid Accounts, API credential abuse), T1190 (Exploit Public-Facing Application), T1530 (Data from Cloud Storage), T1567.002 (Exfiltration Over Web Service), and T1657 (Financial Theft/Extortion). An alleged secondary compromise of Salesforce as an integration vector, per threat actor claims on the extortion site, has not been confirmed by Instructure or Salesforce. The attack pattern

is consistent with prior ShinyHunters operations targeting SaaS platforms via credential stuffing, OAuth token abuse, or misconfigured API endpoints. No patch has been issued; this is a SaaS-layer breach, not a software vulnerability with a client-side fix. Confidence in attribution to ShinyHunters: HIGH. Confidence in 275M record count: LOW. Confidence in Salesforce secondary compromise: LOW.

Action Checklist

1. Containment: Audit all active Canvas API tokens and OAuth integrations immediately. Revoke and rotate any tokens associated with third-party integrations, including any Salesforce-Canvas connectors, pending confirmation of the Salesforce compromise vector. Contact your Instructure account representative to understand whether your institution's tenant was within the confirmed exposure scope.
2. Detection: Review Canvas admin audit logs for anomalous API calls, bulk data export events, or access from unfamiliar IP ranges over the past 90 days. Query your SIEM for Canvas-originated authentication events against known ShinyHunters-associated infrastructure if your threat intelligence feed includes relevant IOCs. Monitor for credential reuse attempts against institutional SSO or identity providers federated with Canvas.
3. Eradication: Reset all Canvas admin and service account credentials. Force password resets for any accounts where Canvas credentials are shared with other systems. Disable any unused API integrations or LTI tools that retain OAuth access to Canvas data. Validate that Salesforce integration credentials are rotated if your environment uses a Canvas-Salesforce connector.
4. Recovery: Confirm with Instructure that your tenant's data is no longer at risk and obtain a written incident scope statement for your records. Validate that MFA is enforced on all Canvas admin accounts and all federated identity provider accounts. Monitor for anomalous login activity and dark web exposure of institutional email addresses using your threat intelligence tooling.
5. Post-Incident: This is Instructure's second incident in eight months. Conduct a formal third-party risk review of Canvas as a critical SaaS dependency. Evaluate data minimization practices: what student PII is stored in Canvas that is not operationally required. Assess whether your institution's data processing agreement with Instructure reflects current breach notification obligations under FERPA and applicable state privacy laws.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate immediately to institutional legal counsel and CISO if Instructure confirms your tenant is within the breach scope, if dark web monitoring surfaces your institutional email domain in ShinyHunters-attributed datasets, or if anomalous Canvas API activity is detected in your audit logs — any of these conditions triggers FERPA breach notification assessment obligations and potential state student privacy law notification requirements.

Recovery Notes	Post-containment, maintain daily review of Canvas authentication logs and IdP sign-in anomaly reports for a minimum of 30 days given that ShinyHunters typically monetizes exfiltrated data through phishing campaigns and credential stuffing within weeks of a breach claim. Verify with Instructure that platform-level controls have been implemented to prevent recurrence before restoring any revoked third-party integrations, and obtain written confirmation of the remediation scope. Given this is Instructure's second incident in eight months, do not restore full integration capabilities until the formal third-party risk review is complete and the Data Processing Agreement has been validated against current breach notification obligations.
Forensic Artifacts	Canvas Authentication Audit Log (Admin > Logging > Authentication): 90-day export showing API token usage, originating IP addresses, user agents, and bulk data access patterns — the primary artifact for identifying whether ShinyHunters accessed your tenant via scripted API harvesting of student records endpoints (/api/v1/users, /api/v1/courses/:id/students, /api/v1/conversations). | Canvas Data 2 (CD2) sync job logs and Snowflake/S3 export records: If your institution uses Canvas Data 2 for data warehouse sync, preserve all job execution logs showing what datasets were exported, when, and to which destination — bulk PII exfiltration at scale from Canvas is most efficiently achieved through the CD2 pipeline or the legacy Canvas Data API. | Federated IdP sign-in logs (Shibboleth SP logs, Azure AD Sign-in logs, or Okta System Log) filtered for Canvas entity/application ID: These logs will surface credential reuse attacks and unauthorized SSO token issuance that may indicate downstream exploitation of exfiltrated Canvas credentials against other institutional systems. | Salesforce Connected App authorization audit trail (Salesforce Setup > Security > Event Monitoring or Setup Audit Trail): If a Canvas-Salesforce integration exists, this log shows OAuth grant history, API call volume from the Canvas integration user, and any anomalous data access patterns during the exposure window — critical for confirming or ruling out the alleged secondary Salesforce compromise vector. | Institutional email gateway or spam filter logs for post-breach phishing indicators: ShinyHunters monetizes student PII through targeted phishing campaigns — logs from your email gateway (Proofpoint, Mimecast, Google Workspace Admin, or Exchange message trace) showing spear-phishing attempts against student/staff email addresses using Canvas-specific lures (e.g., fake Canvas password reset, grade notification) in the weeks following the breach claim are high-value indicators of active exploitation of the exfiltrated dataset.

Per-Action IR Details

Containment — Audit all active Canvas API tokens and OAuth integrations immediately. Revoke and rotate any tokens associated with third-party integrations, including any Salesforce-Canvas connectors, pending confirmation of the Salesforce compromise vector. Contact your Instructure account representative to understand whether your institution's tenant was within the confirmed exposure scope.

NIST Phase: Containment

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

Controls: NIST IR-4 (Incident Handling), NIST AC-2 (Account Management), NIST SC-12 (Cryptographic Key Establishment and Management), CIS 5.1 (Establish and Maintain an Inventory of Accounts), CIS 6.2 (Establish an Access Revoking Process)

Compensating: Export the full Canvas API token list via Canvas REST API: GET /api/v1/accounts/:account_id/authentication_log — authenticate as admin and pipe output to a local JSON file for manual review. Cross-reference token creation timestamps against the 90-day exposure window using Python's json module or jq. For Salesforce-Canvas OAuth connectors, pull the Connected App list from Salesforce Setup > Apps > Connected Apps and manually revoke any Canvas-linked OAuth grants. Document all revoked tokens with timestamps in a shared incident log (Google Sheet or local text file) before revoking to preserve evidence.

Evidence: Before revoking tokens, export and preserve the complete Canvas OAuth token list including token IDs, associated user IDs, creation timestamps, last-used timestamps, and originating IP addresses. Capture Canvas Admin Event Log entries (Admin > Account > Logging) for token creation and API access events covering the full 90-day window. Preserve any Salesforce-side Connected App OAuth grant logs showing authorization timestamps and authorized user accounts for the Canvas integration. Screenshot or export the current Instructure account scope confirmation before any remediation alters the tenant state.

Detection — Review Canvas admin audit logs for anomalous API calls, bulk data export events, or access from unfamiliar IP ranges over the past 90 days. Query your SIEM for Canvas-originated authentication events against known ShinyHunters-associated infrastructure if your threat intelligence feed includes relevant IOCs. Monitor for credential reuse attempts against institutional SSO or identity providers federated with Canvas.

NIST Phase: Detection Analysis

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

Controls: NIST IR-5 (Incident Monitoring), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST AU-2 (Event Logging), NIST SI-4 (System Monitoring), CIS 8.2 (Collect Audit Logs)

Compensating: Without a SIEM, pull Canvas audit logs via the API endpoint GET /api/v1/audit/grade_change/courses/:course_id and GET /api/v1/audit/authentication/users/:user_id and export to CSV. Run a Python script to filter for events where request_user_agent is non-browser (indicating scripted API bulk access) or where ip_address falls outside your institutional IP ranges — compare against your known campus CIDR blocks. For SSO credential reuse detection without EDR, query your IdP (Shibboleth or Azure AD) sign-in logs manually filtering for Canvas entity_id with failed authentication attempts or authentication from IP geolocations inconsistent with your student/staff population. ShinyHunters has historically used residential proxy infrastructure — flag any Canvas API calls from ASNs associated with datacenter or residential proxy providers (check ip-api.com/json/ for ASN lookups, free tier).

Evidence: Capture Canvas Authentication Audit Log exports (Admin > Logging > Authentication) for the full 90-day window before any account resets alter log context. Preserve IdP (Shibboleth, Azure AD, Okta) authentication logs showing Canvas service provider entity ID with attention to bulk authentication patterns, unusual geolocation, or authentication attempts outside business hours at scale. If available, capture WAF or reverse proxy logs for Canvas LMS endpoints showing URI patterns consistent with bulk data harvesting (e.g., repeated GET /api/v1/users, /api/v1/courses/:id/students, or /api/v1/conversations endpoints at high frequency from a single source IP or rotating IP block). Document any ShinyHunters-attributed IOCs from threat intel feeds with timestamps of any matches against your Canvas-origin traffic.

Eradication — Reset all Canvas admin and service account credentials. Force password resets for any accounts where Canvas credentials are shared with other systems. Disable any unused API integrations or LTI tools that retain OAuth access to Canvas data. Validate that Salesforce integration credentials are rotated if your environment uses a Canvas-Salesforce connector.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST IR-4 (Incident Handling), NIST IA-5 (Authenticator Management), NIST CM-7 (Least Functionality), NIST SI-2 (Flaw Remediation), CIS 4.7 (Manage Default Accounts on Enterprise Assets and Software), CIS 5.3 (Disable Dormant Accounts)

Compensating: Enumerate all active Canvas LTI tool configurations via Admin > Settings > Apps and export the list. For each LTI tool retaining OAuth, verify last-used date via Canvas API GET /api/v1/accounts/:account_id/lti_apps — disable any with no activity in 90 days or with no documented business owner. Force admin credential rotation by temporarily disabling and re-enabling admin accounts via Canvas admin panel, which invalidates existing session tokens. For Salesforce credential rotation without automated tooling, manually regenerate the Salesforce API user's security token via Salesforce Setup > My Personal Information > Reset My Security Token and update all dependent Canvas integration configurations. Document each disabled integration and credential rotation with timestamp in your incident log.

Evidence: Before disabling LTI tools and integrations, capture the full list of configured LTI tools with their consumer keys, launch URLs, and OAuth grant scopes — this establishes the pre-incident attack surface for your post-incident review. Preserve Canvas course and account-level external tool configuration exports. Capture Salesforce Connected App audit trail showing authorization history for the Canvas integration user prior to credential rotation. If any LTI tools are flagged as suspicious (unknown vendor, recently added, broad scope), preserve their configuration details as potential evidence of unauthorized integration installation.

Recovery — Confirm with Instructure that your tenant's data is no longer at risk and obtain a written incident scope statement for your records. Validate that MFA is enforced on all Canvas admin accounts and all federated identity provider accounts. Monitor for anomalous login activity and dark web exposure of institutional email addresses using your threat intelligence tooling.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST IR-4 (Incident Handling), NIST IA-3 (Device Identification and Authentication), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST CP-10 (System Recovery and Reconstitution), CIS 6.3 (Require MFA for Externally-Exposed Applications), CIS 6.5 (Require MFA for Administrative Access)

Compensating: Validate Canvas admin MFA enforcement by reviewing Admin > Account > Security Settings for the 'Require Multi-Factor Authentication' policy state. For institutions without commercial dark web monitoring, use HaveIBeenPwned's free domain search (search.haveibeenpwned.com) to check your institutional email domain against known breach databases — note this will not surface the ShinyHunters dataset if it has not yet been submitted to HIBP, but will catch downstream credential reuse. Monitor your IdP sign-in logs daily for 30 days post-containment using a simple export-and-diff script (compare today's unique IP count against a rolling 7-day baseline) to surface anomalous authentication patterns. Request a written scope attestation from Instructure in writing — email with read receipt is sufficient if a formal breach notification letter is not yet available.

Evidence: Capture a baseline export of Canvas admin account list with MFA enrollment status before and after enforcement validation — this documents the pre-recovery MFA gap for regulatory purposes. Preserve the written scope confirmation from Instructure as a dated artifact for FERPA breach notification recordkeeping. Collect a snapshot of IdP authentication volumes (daily unique user count, failure rate, geographic distribution) at recovery initiation to serve as a clean baseline for anomaly detection during the monitoring window.

Post-Incident — This is Instructure's second incident in eight months. Conduct a formal third-party risk review of Canvas as a critical SaaS dependency. Evaluate data minimization practices: what student PII is stored in Canvas that is not operationally required. Assess whether your institution's data processing agreement with Instructure reflects current breach notification obligations under FERPA and applicable state privacy laws.

NIST Phase: Post Incident

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

Controls: NIST IR-4 (Incident Handling), NIST IR-8 (Incident Response Plan), NIST RA-3 (Risk Assessment), NIST SI-12 (Information Management and Retention), NIST CA-2 (Control Assessments), CIS 3.2 (Establish and Maintain a Data Inventory), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process)

Compensating: Conduct the third-party risk review using the free HECVAT Lite questionnaire (Higher Education Community Vendor Assessment Toolkit — available at educause.edu/hecvat) which is specifically designed for higher education SaaS vendor assessments and maps directly to FERPA and NIST 800-171 controls relevant to student PII. For data minimization assessment, export the Canvas data categories via Admin > Data Services > Canvas Data 2 API schema documentation and map each data field to an operational justification — flag fields with no documented educational purpose. Review your existing Data Processing Agreement with Instructure against FERPA 34 CFR Part 99.31(a)(1) school official exception requirements and document any gaps for legal counsel review. Worth noting: FERPA breach notification obligations and applicable state student privacy laws (e.g., NY Education Law 2-d, CA SOPIPA) require human legal verification before any breach notification decisions are finalized.

Evidence: Compile the complete incident timeline from initial detection through recovery as the primary post-incident artifact — include all Canvas audit log exports, Instructure communications, token revocation records, and credential rotation timestamps. Retrieve the previous Instructure incident report from eight months prior and conduct a gap analysis comparing the breach vectors, affected data categories, and Instructure's remediation commitments against this incident's characteristics. Document the current Canvas data retention configuration (Admin > Settings > Reports) to support the data minimization review. Preserve all written communications with Instructure including scope statements and incident notifications as regulatory compliance records under FERPA.

Detection Guidance

Canvas does not provide direct SIEM log forwarding by default; detection depends on what your institution has configured. Check Canvas admin audit logs (Admin > Logging) for bulk data access events, API calls returning large record sets, or access from IP addresses outside your institution's expected ranges. If you have integrated Canvas with a CASB or SSO provider (Okta, Azure AD, Google Workspace), query those logs for anomalous Canvas session activity, token issuance spikes, or API calls outside business hours. Look for outbound data transfers to cloud storage endpoints (T1530, T1567.002) from any systems integrated with Canvas. ShinyHunters has historically used compromised API credentials rather than exploiting a specific software vulnerability, so focus detection on authentication anomalies: failed login spikes, successful logins from new geolocations, and service account activity outside normal patterns. No confirmed IOCs have been publicly attributed to this specific campaign at time of writing; monitor threat intelligence feeds for emerging indicators.

Indicators of Compromise

Type	Value	Context	Confidence
URL	`https://www.bleepingcomputer.com/news/security/instructure-confirms-data-breach-shinyhunters-claims-attack/`	BleepingComputer reporting confirming Instructure breach and ShinyHunters attribution	HIGH
URL	`https://www.instructure.com/resources/blog/security-incident-update`	Official Instructure incident disclosure and update page	HIGH

Framework Mappings

MITRE-ATTACK

- **T1190** — Exploit Public-Facing Application
- **T1657** — Financial Theft
- **T1078** — Valid Accounts
- **T1567.002** — Exfiltration to Cloud Storage
- **T1586.002** — Email Accounts
- **T1530** — Data from Cloud Storage
- **T1567** — Exfiltration Over Web Service

NIST-800-53R5

- **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-2** — Account Management
- **AC-6** — Least Privilege
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **AC-3** — Access Enforcement
- **SC-28** — Protection of Information at Rest

OWASP-TOP10-2021

- **A01:2021** — Broken Access Control
- **A04:2021** — Insecure Design
- **A07:2021** — Identification and Authentication Failures

CIS-V8

- **6.1** — Establish an Access Granting Process
- **6.2** — Establish an Access Revoking Process
- **5.2** — Use Unique Passwords
- **6.3** — Require MFA for Externally-Exposed Applications

SOC2-TSC

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

HIPAA-SECURITY

- **164.312(a)(1)** — Access Control
- **164.308(a)(5)(ii)(D)** — Password Management
- **164.312(d)** — Person or Entity Authentication

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1190	Exploit Public-Facing Application	Initial-Access
T1657	Financial Theft	Impact
T1078	Valid Accounts	Defense-Evasion

Technique ID	Technique Name	Tactic
T1567.002	Exfiltration to Cloud Storage	Exfiltration
T1586.002	Email Accounts	Resource-Development
T1530	Data from Cloud Storage	Collection
T1567	Exfiltration Over Web Service	Exfiltration

Sources

Source	URL	Tier
Security News	https://www.bleepingcomputer.com/news/security/instructure-confirms...	T3
Edu tech firm Instructure discloses cyber incident, probes impact	https://www.bleepingcomputer.com/news/security/edu-tech-firm-instru...	T3
Instructure Canvas Discloses Second Cybersecurity Incident i	https://techjacksolutions.com/scc-intel/instructure-canvas-disclose...	T3
Instructure Canvas Breach: Second Hit in 8 Months Exposes Student ...	https://www.gblock.app/articles/instructure-canvas-may-2026-breach-...	T3
Update on Security Incident - Instructure	https://www.instructure.com/resources/blog/security-incident-update	T3

Generated 2026-05-04 06:06 UTC by TJS Security Command Center