INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-05-02 06:45 UTC

Instructure Canvas Discloses Second Cybersecurity Incident in Eight Months Amid Ongoing Investigation

DATA BREACH | HIGH | CVSS 5.0

SCC Item ID	SCC-DBR-2026-0108
Type	Data Breach
Severity	HIGH
CVSS Base Score	5.0
Affected Products	Instructure Canvas LMS, Canvas Data 2, Canvas Beta
Published	2026-05-01T19:43:35
Discovery Source	Rss

Executive Summary

Instructure, the company behind Canvas LMS, disclosed a cybersecurity incident on May 1, 2026, placing Canvas Data 2 and Canvas Beta into maintenance mode amid an active investigation. The affected platform is used by millions of students and educators globally; potential exposure of personally identifiable information has not been confirmed or ruled out. This is the second incident in eight months, indicating sustained targeting of Instructure's infrastructure and elevating concerns about data stewardship across the education technology sector.

Technical Analysis

Instructure disclosed an active cybersecurity incident affecting Canvas LMS, Canvas Data 2, and Canvas Beta as of May 1, 2026. Root cause has not been confirmed; no CVE has been assigned. Suspected vulnerability classes based on incident characteristics are CWE-306 (Missing Authentication for Critical Function), CWE-287 (Improper Authentication), and CWE-359 (Exposure of Private Personal Information to an Unauthorized Actor). MITRE ATT&CK techniques associated with this incident pattern include T1566 (Phishing), T1199 (Trusted Relationship), T1530 (Data from Cloud Storage), T1657 (Financial Theft), T1213 (Data from Information Repositories), T1190 (Exploit Public-Facing Application), T1486 (Data Encrypted for Impact), and T1078 (Valid Accounts). ShinyHunters has been surfaced as a suspected threat actor; no official attribution has been established. Canvas Data 2 and Canvas Beta entered maintenance mode concurrent with disclosure, suggesting operational disruption beyond initial scope. External forensic investigators are engaged. No patch, vendor advisory with remediation steps, or confirmed attack vector has been published as of disclosure. CVSS

base score and vendor scoring are pending official NVD and vendor publication. Source quality score is 0.56, reflecting early-stage reporting.

Action Checklist

1. Step 1: Containment. Audit all active Canvas LMS, Canvas Data 2, and Canvas Beta integrations in your environment. Temporarily restrict API access and third-party integrations to Canvas until Instructure confirms the attack vector and scope. Review Canvas OAuth tokens and API keys issued in the last 90 days; revoke any that cannot be attributed to a known authorized application or user.
2. Step 2: Detection. Review identity and access logs for Canvas for anomalous authentication events, including logins from unexpected geographic locations, off-hours access, or service account activity outside normal patterns. Canvas audit logs (if enabled via institution admin console) should be pulled for the period surrounding May 1, 2026. Monitor for bulk data export events from Canvas Data 2. No confirmed IOC patterns are available from official sources as of this item's disclosure date.
3. Step 3: Eradication. No confirmed patch or remediation guidance has been published by Instructure. Monitor the Instructure security blog (https://www.instructure.com/resources/blog/security-incident-update) for official remediation steps. If CWE-287 or CWE-306 are confirmed, priority remediation will likely involve authentication configuration hardening and MFA enforcement on all Canvas admin and API accounts.
4. Step 4: Recovery. Once Instructure publishes root cause and remediation guidance, validate that all Canvas API credentials, OAuth tokens, and admin accounts have been rotated. Confirm Canvas Data 2 pipeline integrity before resuming any automated data exports. Re-enable suspended integrations only after verifying they were not part of the attack path.
5. Step 5: Post-Incident. Evaluate your institution's dependency on Canvas Data 2 for data pipeline continuity planning. Review third-party app integrations authorized in your Canvas environment against a principle-of-least-privilege baseline. If PII exposure is confirmed, initiate your data breach notification assessment process per applicable state, national, or institutional policy. Document findings for the next security review cycle.

IR / Forensic Enrichment

Triage Priority	URGENT
Escalation Criteria	Escalate immediately to institutional legal counsel, privacy officer, and CISO if Instructure confirms PII exfiltration from Canvas Data 2 or Canvas LMS user records, as FERPA notification obligations and applicable state breach notification statutes (which vary by jurisdiction but commonly require notification within 30–72 hours) would be triggered; also escalate if internal log review identifies Canvas admin account compromise or unauthorized bulk data exports from your institution's Canvas environment independent of Instructure's investigation.

Recovery Notes	Do not resume Canvas Data 2 automated pipeline exports until Instructure has published a confirmed root cause and your institution has independently verified that no unauthorized OAuth clients or API keys remain active in your developer key inventory. Given this is Instructure's second incident in eight months, maintain elevated monitoring of Canvas authentication audit logs and Canvas Data 2 job history for a minimum of 60 days post-Instructure remediation confirmation, watching specifically for service account authentications from unexpected IP ranges or off-schedule bulk export jobs. Treat the prior incident's timeframe as a secondary investigation window — review whether any anomalous access patterns present in the current incident also appeared during the prior incident, as this would indicate a persistent access mechanism that survived the first remediation.
Forensic Artifacts	Canvas Authentication Audit Log (GET /api/v1/audit/authentication/logins): captures OAuth client_id, user_id, pseudonym_id, IP address, country_code, and created_at timestamp — the primary source for identifying unauthorized API client activity or anomalous admin logins surrounding May 1, 2026 | Canvas Developer Keys export (admin console or GET /api/v1/developer_keys): documents all OAuth 2.0 client credentials and API tokens issued to third-party integrations; abnormal entries or tokens with no attributable owner are a direct indicator of unauthorized API access in a Canvas-specific breach | Canvas Data 2 job execution history (available in your institution's data warehouse or Canvas Data 2 admin interface): records which accounts triggered data export jobs, the tables exported, row counts, and destination endpoints — critical for scoping potential PII exfiltration from the Canvas Data 2 pipeline specifically called out in this incident | Canvas LTI integration redirect URIs and launch URL configurations (GET /api/v1/accounts/:account_id/lti_apps): a compromised LTI tool registration is a plausible lateral vector in a Canvas breach; mismatched or newly-added redirect_uri values against known vendor documentation indicate potential OAuth redirect hijacking consistent with CWE-287 | Institution IdP (SSO) authentication logs for Canvas service provider entity: if your institution uses SAML or OIDC for Canvas authentication, the IdP-side logs (Shibboleth, Azure AD, Okta) will contain authentication assertions that Canvas-side audit logs may not fully capture — cross-correlating IdP assertion timestamps with Canvas audit login events can identify forged or replayed authentication tokens consistent with CWE-306 (Missing Authentication for Critical Function)

Per-Action IR Details

Step 1: Containment — Audit all active Canvas LMS, Canvas Data 2, and Canvas Beta integrations in your environment. Temporarily restrict API access and third-party integrations to Canvas until Instructure confirms the attack vector and scope. Review Canvas OAuth tokens and API keys issued in the last 90 days; revoke any that cannot be attributed to a known authorized application or user.

NIST Phase: Containment

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

Controls: NIST IR-4 (Incident Handling), NIST AC-2 (Account Management), NIST AC-17 (Remote Access), CIS 5.1 (Establish and Maintain an Inventory of Accounts), CIS 6.2 (Establish an Access Revoking Process)

Compensating: Export the full OAuth token and API key inventory from your Canvas institution admin console under Account > Developer Keys; pipe the JSON output to a spreadsheet and cross-reference each client_id against your authorized app registry. For tokens with no matching owner, use the Canvas API endpoint GET /api/v1/audit/authentication/logins?per_page=100 with your admin token to pull the last 90 days of authentication events associated with that client_id. Revoke unattributed tokens immediately via DELETE /api/v1/developer_keys/:id. This is achievable by one analyst with curl or Postman in under two hours.

Evidence: Before revoking tokens, capture the full Canvas Developer Keys list (admin console export or API dump) and the Canvas Authentication Audit Log for the 90-day window preceding May 1, 2026. Preserve timestamps, client_id values, and associated user or service account identifiers. This establishes which OAuth clients were active

during the incident window and provides the baseline for determining whether any third-party LTI integration or Canvas Data 2 pipeline connector was used as an entry or exfiltration vector.

Step 2: Detection — Review identity and access logs for Canvas for anomalous authentication events, including logins from unexpected geographic locations, off-hours access, or service account activity outside normal patterns. Canvas audit logs (if enabled via institution admin console) should be pulled for the period surrounding May 1, 2026. Monitor for bulk data export events from Canvas Data 2. No confirmed IOC patterns are available from official sources as of this item's disclosure date.

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-12 (Audit Record Generation), NIST SI-4 (System Monitoring), CIS 8.2 (Collect Audit Logs)

Compensating: Pull Canvas audit logs via the Canvas API: GET /api/v1/audit/authentication/logins and GET /api/v1/audit/grade_change/courses/:course_id for the April 15 – May 10, 2026 window. Pipe output to jq and filter for login events where pseudonym_id differs from historical baseline or where created_at timestamps fall between 00:00–05:00 institution local time. For Canvas Data 2 bulk export monitoring, query your institution's Canvas Data 2 job history table (cd2_requests or equivalent in your data warehouse) for export jobs initiated by service accounts outside scheduled pipeline windows. If your institution uses Splunk Free or Elastic Free tier, load the JSON audit exports and alert on event_type='login' with country_code != your expected country.

Evidence: Capture Canvas Authentication Audit Log entries (event_type, pseudonym_id, user_id, created_at, ip_address, country_code) for April 1 – May 10, 2026. Separately capture Canvas Data 2 job execution logs showing which accounts triggered data exports, export scope (table names, row counts), and destination endpoints. Given this is the second incident in eight months, also pull the equivalent log window from the prior incident period for pattern comparison. Preserve raw JSON before any log rotation occurs — Canvas audit log retention is institution-configurable and may be short.

Step 3: Eradication — No confirmed patch or remediation guidance has been published by Instructure. Monitor the Instructure security blog (https://www.instructure.com/resources/blog/security-incident-update) for official remediation steps. If CWE-287 or CWE-306 are confirmed, priority remediation will likely involve authentication configuration hardening and MFA enforcement on all Canvas admin and API accounts.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST SI-2 (Flaw Remediation), NIST IA-5 (Authenticator Management), NIST IA-8 (Identification and Authentication — Non-Organizational Users), CIS 6.3 (Require MFA for Externally-Exposed Applications), CIS 6.5 (Require MFA for Administrative Access), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: Without waiting for Instructure's root cause, harden now against CWE-287 (Improper Authentication) and CWE-306 (Missing Authentication for Critical Function) proactively: (1) In Canvas admin console, navigate to Account > Authentication and enforce MFA for all admin roles and any account with API token generation privileges. (2) Rotate all Canvas admin account passwords and force re-enrollment of MFA factors. (3) Disable the Canvas Beta environment at the institution level if your institution does not actively use it for testing, as it was specifically placed in maintenance mode and represents an unconfirmed attack surface. (4) Set a calendar reminder to check https://www.instructure.com/resources/blog for updates every 24 hours until official remediation guidance is published — note this URL has not been independently verified as of this response and should be confirmed against the official Instructure site.

Evidence: Before hardening authentication configuration, export the current Canvas authentication provider settings (SAML, LDAP, or native Canvas auth configuration) from Account > Authentication as a baseline. Document which admin accounts currently lack MFA enrollment by running GET /api/v1/accounts/:account_id/admins and cross-referencing against your IdP MFA enrollment report. This documents the pre-remediation authentication posture and supports a post-remediation comparison to confirm hardening was effective.

Step 4: Recovery — Once Instructure publishes root cause and remediation guidance, validate that all Canvas API credentials, OAuth tokens, and admin accounts have been rotated. Confirm Canvas Data 2 pipeline integrity before resuming any automated data exports. Re-enable suspended integrations only after verifying they were not part of the attack path.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST IR-4 (Incident Handling), NIST SI-7 (Software, Firmware, and Information Integrity), NIST CP-10 (System Recovery and Reconstitution), NIST AU-9 (Protection of Audit Information), CIS 7.2 (Establish and Maintain a Remediation Process), CIS 5.1 (Establish and Maintain an Inventory of Accounts)

Compensating: Before re-enabling Canvas Data 2 pipelines, run a row-count and schema-hash comparison between your last known-good data warehouse snapshot (pre-April 2026) and the current state. Use a SQL query against your data warehouse: SELECT table_name, COUNT(*) FROM canvas_data_2_tables GROUP BY table_name and compare against a saved baseline. For OAuth token rotation verification, re-run the GET /api/v1/developer_keys inventory and confirm no client_id values match the pre-rotation list. For each LTI integration being re-enabled, verify the tool's redirect_uri and launch URL against the vendor's current published documentation before restoring.

Evidence: Before resuming Canvas Data 2 exports, capture a hash of your current data warehouse tables for the most sensitive datasets (user PII tables, enrollment records, grade tables) using md5sum or sha256sum on exported CSVs, and compare against pre-incident baselines. This detects whether any unauthorized data modification occurred during the incident window — relevant because the attack vector and whether data was modified (not just exfiltrated) remains unconfirmed as of this disclosure.

Step 5: Post-Incident — Evaluate your institution's dependency on Canvas Data 2 for data pipeline continuity planning. Review third-party app integrations authorized in your Canvas environment against a principle-of-least-privilege baseline. If PII exposure is confirmed, initiate your data breach notification assessment process per applicable state, national, or institutional policy. Document findings for the next security review cycle.

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 AU-11 (Audit Record Retention), CIS 3.2 (Establish and Maintain a Data Inventory), CIS 3.3 (Configure Data Access Control Lists), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: Conduct a scoped LTI and API integration audit using the Canvas API: GET /api/v1/accounts/:account_id/lti_apps and GET /api/v1/developer_keys?per_page=100, then map each integration's data scope (what Canvas data fields it can access) against documented business need. Flag any integration with access to PII fields (email, SIS ID, enrollment data) that lacks a current data processing agreement. For breach notification scoping, query your Canvas SIS integration to enumerate the total count of active user records with email addresses — this establishes the notification population if PII exposure is confirmed. This is achievable with Canvas API access and a spreadsheet in one analyst-day.

Evidence: Retain all Canvas audit log exports, API key inventory snapshots, authentication event logs, and Canvas Data 2 job history logs from the investigation window for a minimum of 12 months per NIST AU-11 (Audit Record Retention). Given this is the second incident in eight months, these records will be critical for identifying whether the same initial access vector was reused. If PII exposure is confirmed, these logs will also constitute required evidence for breach notification documentation under applicable regulations (FERPA, state data breach statutes).

Detection Guidance

No confirmed IOCs are available as of the May 1, 2026 disclosure. Detection focus areas based on suspected CWEs and associated MITRE techniques: (1) Canvas admin and API authentication logs, look for successful

logins without MFA, logins from unrecognized IP ranges, or service account logins outside business hours. (2) Canvas Data 2 pipeline logs, look for unexpected data export jobs, schema access outside normal schedules, or API calls from unrecognized clients. (3) Identity provider (IdP) logs for Canvas SSO, look for token issuance spikes or session anomalies tied to Canvas service accounts. (4) If your institution uses a SIEM, create an alert for Canvas API calls originating from IPs not on your known integration list. (5) Monitor Instructure's official update page and BleepingComputer coverage for IOC releases as the investigation progresses. Given ShinyHunters' historical tactics (credential theft, cloud storage data exfiltration), prioritize review of cloud storage access logs for any Canvas-connected storage buckets or data warehouse endpoints.

Framework Mappings

MITRE-ATTACK

- **T1566** — Phishing
- **T1199** — Trusted Relationship
- **T1530** — Data from Cloud Storage
- **T1657** — Financial Theft
- **T1213** — Data from Information Repositories
- **T1190** — Exploit Public-Facing Application
- **T1486** — Data Encrypted for Impact
- **T1078** — Valid Accounts

NIST-800-53R5

- **AT-2** — Literacy Training and Awareness
- **CA-7** — Continuous Monitoring
- **SC-7** — Boundary Protection
- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **SI-8** — Spam Protection
- **CA-8** — Penetration Testing
- **RA-5** — Vulnerability Monitoring and Scanning
- **SI-2** — Flaw Remediation
- **SI-7** — Software, Firmware, and Information Integrity
- **CP-9** — System Backup
- **CP-10** — System Recovery and Reconstitution
- **AC-2** — Account Management
- **AC-6** — Least Privilege
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **IA-8** — Identification and Authentication (Non-Organizational Users)

OWASP-TOP10-2021

- **A07:2021** — Identification and Authentication Failures

CIS-V8

- **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

HIPAA-SECURITY

- **164.312(d)** — Person or Entity Authentication

ISO-27001-2022

- **A.8.8** — Management of technical vulnerabilities

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1566	Phishing	Initial-Access
T1199	Trusted Relationship	Initial-Access
T1530	Data from Cloud Storage	Collection
T1657	Financial Theft	Impact
T1213	Data from Information Repositories	Collection
T1190	Exploit Public-Facing Application	Initial-Access
T1486	Data Encrypted for Impact	Impact
T1078	Valid Accounts	Defense-Evasion

Sources

Source	URL	Tier
Security News	https://www.bleepingcomputer.com/news/security/edu-tech-firm-instru...	T3
Edu tech firm Instructure discloses cyber incident, probes impact	https://www.bleepingcomputer.com/news/security/edu-tech-firm-instru...	T3

Source	URL	Tier
Vulnerability in canvas-lms project · Issue #2618 - GitHub	https://github.com/instructure/canvas-lms/issues/2618	T3
Update on Security Incident - Instructure	https://www.instructure.com/resources/blog/security-incident-update	T3
Instructure Canvas Learning Management Service security ...	https://www.cvedetails.com/product/92336/Instructure-Canvas-Learnin...	T3

Generated 2026-05-02 06:45 UTC by TJS Security Command Center