INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-05-05 08:36 UTC

Instructure Canvas LMS Data Breach Affects Millions of K-12 Students Across 9,000+ Schools

DATA BREACH | HIGH | CVSS 7.5

SCC Item ID	SCC-DBR-2026-0113
Type	Data Breach
Severity	HIGH
CVSS Base Score	7.5
Affected Products	Instructure Canvas LMS, grades 4-12 students across approximately 9,000 schools; Wayzata Public Schools (Minnesota) confirmed affected
Published	15 hours ago
Discovery Source	Serper

Executive Summary

Threat actors claim to have obtained personal information belonging to approximately 275 million users from Instructure's Canvas learning management system, affecting students across more than 9,000 schools. Wayzata Public Schools in Minnesota has formally notified parents of affected students in grades 4 through 12. The breach claim has not been independently confirmed by Instructure or CISA; however, the scale of the claim and the involvement of minors' data represent significant legal, regulatory, and reputational exposure for affected districts and their technology vendors.

Technical Analysis

Reported breach involves Instructure Canvas LMS with threat actors claiming unauthorized access to PII for approximately 275 million users across 9,000-plus educational institutions. Breach vector has not been confirmed in available sources. Relevant weaknesses align with CWE-200 (Exposure of Sensitive Information to an Unauthorized Actor) and CWE-359 (Exposure of Private Personal Information to an Unauthorized Actor). MITRE ATT&CK techniques T1530 (Data from Cloud Storage) and T1078 (Valid Accounts) are consistent with cloud-hosted LMS compromise patterns, though neither technique has been confirmed as the actual vector for this incident. No CVE has been assigned. No patch or vendor advisory from Instructure has been confirmed in available sources as of the item date. Source quality is limited to T3 news reporting (FOX9, Yahoo News); no authoritative technical confirmation from Instructure or CISA is available. All technical attribution should be treated as unverified until Instructure issues a formal disclosure.

Action Checklist

1. Containment. Determine immediately whether your district or organization uses Canvas as a primary or integrated LMS. Contact your Instructure account representative or district IT point of contact to request confirmation of whether your tenant data was included in the claimed breach scope.

2. Detection. Review access logs for your Canvas tenant (available via Canvas Data Services or your SIS integration logs) for anomalous API calls, bulk data exports, or OAuth token activity outside normal patterns. Correlate against T1078 (Valid Accounts) by auditing admin-level and integration-level account activity in the 90-day window preceding this report.

3. Eradication. No vendor-confirmed patch or remediation advisory is available as of the item date. Pending official guidance: rotate all Canvas API tokens and OAuth credentials, disable unused third-party integrations, and enforce re-authentication for all admin accounts. Do not wait for vendor confirmation before rotating credentials.

4. Recovery. Once Instructure issues a formal advisory, validate your tenant's exposure scope against disclosed data fields. Review your Student Information System (SIS) sync configurations to identify which PII fields were transmitted to Canvas. Confirm multi-factor authentication is enforced on all Canvas admin and instructor accounts.

5. Post-Incident. This incident highlights control gaps common to cloud-hosted EdTech platforms: insufficient vendor contractual obligations for breach notification timelines, lack of data minimization in LMS-SIS integrations, and absent or immature FERPA-aligned data handling audits. Initiate a vendor risk review of all cloud LMS and EdTech integrations, specifically evaluating data retention, export controls, and breach notification SLAs.

IR / Forensic Enrichment

Triage Priority	URGENT
Escalation Criteria	Escalate immediately to district legal counsel, the student data privacy officer, and state education agency if Instructure formally confirms that your tenant's student PII was included in the breach, if any Canvas API logs show bulk export activity matching T1078 patterns in the 90-day review window, or if affected students include any under age 13 (triggering COPPA obligations in addition to FERPA); state breach notification deadlines for minors' educational records vary by jurisdiction and typically require notification within 30-72 hours of confirmed breach.
Recovery Notes	After credential rotation and MFA enforcement are confirmed, monitor Canvas Data Services 'requests' table daily for 30 days for any resumption of anomalous bulk API calls to user enumeration endpoints, paying particular attention to any OAuth app IDs that were active during the suspected breach window but were not deleted during eradication. Validate that SIS sync resumes normally post-rotation by confirming successful nightly sync jobs and reviewing SIS Import History for error codes that could indicate credential misconfiguration. Do not reduce monitoring cadence until Instructure issues a formal advisory confirming breach scope and remediation completeness; the unconfirmed status of this breach means the threat actor's access method and persistence mechanisms remain unknown.

Forensic Artifacts	Canvas Data Services 'requests' table: HTTP GET requests to /api/v1/accounts/*/users, /api/v1/courses/*/students, and /api/v1/users/* endpoints with HTTP 200 responses — these are the specific API paths required for bulk student PII enumeration at the scale claimed (275M records); filter for high-frequency calls from a single OAuth client_id or IP range over the 90-day window | Canvas Developer Keys audit log: records of OAuth token creation, last_used_at timestamps, and associated redirect_uri values — a threat actor performing a large-scale API harvest would require a valid OAuth token, and any token with an unrecognized redirect_uri or created outside a change management window is a high-priority indicator | Canvas SIS Import History (Admin > SIS Import > Past Imports): log of all inbound SIS sync jobs including file hash, submitting account, and record counts — an unexpected or unauthorized SIS import could indicate an attempt to manipulate or exfiltrate student enrollment data via the sync mechanism | Canvas 'pseudonym_dim' table from Canvas Data Services: login records including authentication provider type (SAML vs. canvas native), last_request_at, and IP address for all accounts with admin or sub-account admin roles — used to identify admin account activity during the suspected breach window, specifically logins from IPs outside the district's known IP ranges or during off-hours consistent with threat actor dwell time | SIS connector audit logs (PowerSchool Plugin Logs, Infinite Campus Canvas Rostering export logs, or Clever sync logs): outbound data exports from the SIS to Canvas showing exactly which student PII fields were transmitted and when — this is the ground-truth record of what data was in Canvas at the time of the alleged breach and is required for any FERPA parent notification that must specify categories of information disclosed

Per-Action IR Details

Containment — Determine immediately whether your district or organization uses Canvas as a primary or integrated LMS. Contact your Instructure account representative or district IT point of contact to request confirmation of whether your tenant data was included in the claimed breach scope.

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 — Containment Strategy: Identify the scope of affected systems and data before executing containment actions to avoid disrupting unaffected components.

Controls: NIST IR-4 (Incident Handling), NIST IR-6 (Incident Reporting), NIST RA-2 (Security Categorization) — categorize the Canvas tenant as a high-value asset given it stores FERPA-protected minor PII, CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory) — confirm Canvas is documented as an enterprise asset with known data flows, CIS 3.2 (Establish and Maintain a Data Inventory) — identify which PII fields your district SIS sync transmits to Canvas

Compensating: Without a vendor-managed CSAM tool, query your SIS (PowerSchool, Infinite Campus, or equivalent) for active Canvas API integration records. Run: curl -H 'Authorization: Bearer ' https://.instructure.com/api/v1/accounts/self/sub_accounts to enumerate active tenants. Document Canvas subdomain, SIS sync account, and all OAuth app registrations in a spreadsheet before contacting Instructure — this accelerates scope confirmation.

Evidence: Before initiating vendor contact, snapshot the current state of your Canvas tenant: export the list of active OAuth applications via Canvas Admin > Developer Keys, capture a timestamped screenshot of all SIS integration sync logs under Admin > SIS Import > Import History, and record all active Canvas Data Services (CDS) export jobs. This establishes a pre-communication baseline in case Instructure's advisory changes tenant-level details after notification.

Detection — Review access logs for your Canvas tenant (available via Canvas Data Services or your SIS integration logs) for anomalous API calls, bulk data exports, or OAuth token activity outside normal patterns. Correlate against T1078 (Valid Accounts) by auditing admin-level and integration-level account activity in the 90-day window preceding this report.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis: Correlate indicators across multiple log sources and apply threat intelligence context (MITRE T1078 Valid Accounts) to distinguish malicious API abuse from legitimate automation.

Controls: NIST AU-2 (Event Logging) — confirm Canvas API access logging is enabled in Canvas Data Services, NIST AU-6 (Audit Record Review, Analysis, and Reporting) — perform structured review of Canvas access logs over the 90-day window, NIST SI-4 (System Monitoring) — monitor for anomalous OAuth token issuance and bulk data export API calls specific to Canvas, NIST IR-5 (Incident Monitoring) — track and document all anomalous Canvas API events as potential incident indicators, CIS 8.2 (Collect Audit Logs) — ensure Canvas Data Services logs and SIS sync logs are collected and retained, MITRE ATT&CK T1078 (Valid Accounts) — adversaries may have used compromised Canvas admin or integration service accounts to perform bulk PII exports

Compensating: Canvas Data Services (CDS) exports raw event tables including requests, user_dim, and pseudonym_dim. Download the requests table for the 90-day window and run this Python one-liner to flag bulk export behavior: python3 -c "import csv,sys; [print(r) for r in csv.DictReader(open('requests.csv')) if r.get('http_method')=='GET' and '/api/v1/users' in r.get('url','') and int(r.get('http_status','0'))==200]" . Flag any OAuth client_id appearing in >500 API calls per day or any admin account triggering /api/v1/accounts//users or /api/v1/courses//students endpoints in bulk. Cross-reference OAuth app IDs against your Developer Keys inventory captured in the containment step.

Evidence: Collect before analysis: (1) Canvas Data Services 'requests' table filtered for HTTP 200 responses to /api/v1/users, /api/v1/courses/*/students, /api/v1/accounts/*/users endpoints — these are the API paths a threat actor would use to enumerate student PII at scale. (2) Canvas 'pseudonym_dim' table showing login events, pseudonym type (SAML vs. canvas), and last_request_at timestamps for all admin and integration accounts. (3) SIS Import History export showing all inbound sync jobs — look for unexpected SIS imports that may have been used to inject or exfiltrate data. (4) Developer Keys audit log showing when each OAuth token was created, last used, and by which IP range.

Eradication — No vendor-confirmed patch or remediation advisory is available as of the item date. Pending official guidance: rotate all Canvas API tokens and OAuth credentials, disable unused third-party integrations, and enforce re-authentication for all admin accounts. Do not wait for vendor confirmation before rotating credentials.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication: Remove threat actor footholds including compromised credentials and unauthorized persistent access mechanisms before beginning recovery, even absent vendor confirmation.

Controls: NIST IR-4 (Incident Handling) — execute eradication actions consistent with the incident response plan without waiting for vendor advisory when credential compromise is suspected, NIST AC-2 (Account Management) — audit and remediate all Canvas admin, instructor, and integration service accounts, NIST IA-5 (Authenticator Management) — rotate all Canvas API tokens, OAuth client secrets, and SIS integration credentials immediately, NIST CM-7 (Least Functionality) — disable all Canvas third-party LTI integrations and OAuth apps that are not actively in use, CIS 5.3 (Disable Dormant Accounts) — disable any Canvas admin or integration accounts inactive for 45+ days, CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts) — audit Canvas admin role assignments and remove excess admin grants, MITRE ATT&CK T1078 (Valid Accounts) — credential rotation invalidates any session tokens or API keys a threat actor may have harvested

Compensating: Using Canvas Admin UI (no SIEM required): (1) Navigate to Admin > Developer Keys — delete all keys with last_used_at older than 30 days or with unknown owner. (2) Navigate to Admin > Admins — export the full admin list, cross-reference against HR-confirmed active staff, and remove excess. (3) For SIS integration credentials, regenerate the Canvas SIS import token in Admin > Settings > Integrations and update the SIS connector (PowerSchool, Infinite Campus) immediately. (4) Force global re-authentication by navigating to Admin > Settings and enabling 'Expire Sessions' — this invalidates all active session cookies. Document every action with timestamp and operator name for the incident record.

Evidence: Before rotating credentials, capture: (1) A full export of Developer Keys (Canvas Admin > Developer Keys > export) showing all OAuth apps, their last_used_at timestamps, and associated redirect URIs — a threat actor may have registered a malicious OAuth app to maintain persistence. (2) The current admin account list with role assignments from Admin > Admins. (3) Any Canvas webhook configurations under Admin > Settings > Web Hooks — webhooks pointing to external URLs could be exfiltration channels. Preserve these records before rotation so

post-incident analysis can identify which credentials were active during the suspected breach window.

Recovery — Once Instructure issues a formal advisory, validate your tenant's exposure scope against disclosed data fields. Review your Student Information System (SIS) sync configurations to identify which PII fields were transmitted to Canvas. Confirm multi-factor authentication is enforced on all Canvas admin and instructor accounts.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery: Restore systems to normal operation only after validating that threat actor access has been eliminated and implementing hardening to prevent recurrence.

Controls: NIST IR-4 (Incident Handling) — validate recovery steps against the incident response plan, including confirmation that MFA is enforced prior to restoring normal operations, NIST IA-3 (Device Identification and Authentication) — enforce MFA for all Canvas admin and instructor accounts via SAML/SSO provider or Canvas native MFA, NIST AC-3 (Access Enforcement) — review Canvas role-based access to confirm students cannot access other students' PII via Canvas API or Data Services, NIST SI-7 (Software, Firmware, and Information Integrity) — verify SIS sync configuration integrity to confirm no unauthorized field mappings were introduced, CIS 6.3 (Require MFA for Externally-Exposed Applications) — Canvas is an externally-exposed SaaS LMS; MFA must be enforced for all accounts, not just admins, CIS 6.5 (Require MFA for Administrative Access) — prioritize MFA enforcement for Canvas admin and sub-account admin roles, CIS 3.2 (Establish and Maintain a Data Inventory) — document which specific PII fields (student name, DOB, grade, SIS ID, email, parent contact) are included in the SIS-to-Canvas sync

Compensating: Without an enterprise IAM platform: (1) Enable MFA in Canvas natively via Admin > Authentication > Add Authentication Provider > select your SSO provider (Google, Microsoft, SAML) and enforce MFA at the IdP level. (2) Audit SIS sync field mappings by reviewing your SIS connector configuration — in PowerSchool, check the Canvas plugin data export definition; in Infinite Campus, review the Canvas Rostering export fields. Produce a written inventory of every PII field synced (student_id, email, grade_level, guardian_email, etc.) and compare against what Instructure discloses in their advisory. (3) Use Canvas's built-in 'Course Analytics' and 'Admin Analytics' (free, no third-party tool required) to confirm no abnormal data access resumes post-recovery.

Evidence: Before declaring recovery complete, collect: (1) MFA enforcement confirmation — export your IdP sign-in logs (Google Workspace Admin, Azure AD, or Okta) showing MFA challenges for Canvas SSO logins post-rotation. (2) SIS sync field inventory document listing every attribute transmitted to Canvas, with the data classification (directory vs. non-directory FERPA data) for each. (3) Canvas 'pseudonym_dim' snapshot post-rotation confirming all pre-rotation session tokens are invalidated (last_request_at on old pseudonyms should not advance after rotation date). This evidence supports both recovery validation and any required FERPA breach notification documentation.

Post-Incident — This incident highlights control gaps common to cloud-hosted EdTech platforms: insufficient vendor contractual obligations for breach notification timelines, lack of data minimization in LMS-SIS integrations, and absent or immature FERPA-aligned data handling audits. Initiate a vendor risk review of all cloud LMS and EdTech integrations, specifically evaluating data retention, export controls, and breach notification SLAs.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity: Document lessons learned, update policies, and improve vendor oversight controls to reduce recurrence risk from third-party EdTech data handling gaps.

Controls: NIST IR-4 (Incident Handling) — update the incident handling capability to include a vendor-managed SaaS LMS breach scenario based on this incident, NIST IR-8 (Incident Response Plan) — revise the IR plan to include Canvas-specific and EdTech-specific playbook entries with FERPA breach notification decision trees, NIST SA-9 (External System Services) — establish or revise Instructure contractual requirements for breach notification timelines, data retention limits, and audit log access SLAs, NIST RA-3 (Risk Assessment) — conduct a formal risk assessment of all SaaS EdTech vendors with access to student PII, prioritizing those with SIS integrations, NIST SI-12 (Information Management and Retention) — require Instructure and other EdTech vendors to document and enforce data retention and deletion schedules for student PII, CIS 7.1 (Establish and Maintain a Vulnerability Management Process) — extend vulnerability management process to include third-party SaaS vendor security posture reviews, CIS 3.4 (Enforce Data Retention) — apply data retention controls to EdTech vendor contracts, specifying maximum PII

retention windows aligned to FERPA requirements, CIS 3.2 (Establish and Maintain a Data Inventory) — update the data inventory to reflect all PII fields shared with Canvas and other EdTech SaaS platforms

Compensating: Without a dedicated vendor risk management platform: (1) Create a standardized EdTech Vendor Risk Worksheet (spreadsheet) capturing for each vendor: PII fields received, FERPA data classification, breach notification SLA in contract, data retention period, MFA enforcement status, and last security review date. Populate this for Canvas first, then all other LTI/SIS-integrated tools. (2) Use CISA's Free Cybersecurity Services and Tools catalog and CoSN's (Consortium for School Networking) EdTech data privacy resources — both are free and provide K-12-specific vendor assessment frameworks. (3) Submit a formal data processing questionnaire to Instructure referencing FERPA 34 CFR §99.31 and request their current Data Processing Agreement (DPA) — this is standard practice and most vendors will respond. Document all requests and responses in the incident record.

Evidence: For the post-incident record, preserve: (1) The current Instructure Data Processing Agreement (DPA) and Master Service Agreement (MSA) — specifically the breach notification clause and data retention schedule — as baseline for contract remediation. (2) The full SIS-to-Canvas PII field inventory created during recovery (see Recovery step evidence). (3) A timestamped log of all communications with Instructure regarding this breach claim, including dates, contact names, and responses — this is required documentation if FERPA breach notification to parents becomes necessary. (4) The complete list of all third-party LTI tools and OAuth integrations active in your Canvas tenant at the time of the incident, as these represent additional exposure vectors for the same dataset.

Detection Guidance

No confirmed IOCs are available from authoritative sources. Detection efforts should focus on behavioral indicators consistent with T1530 and T1078. In Canvas audit logs (accessible via the Canvas Data Services pipeline or REST API audit endpoints), look for: bulk enrollment data exports outside business hours; API calls from unfamiliar IP ranges accessing user profile or SIS data endpoints; OAuth token grants to unrecognized third-party applications; admin account logins from unusual geolocations or user agents. In your SIS integration logs, flag unexpected outbound data pulls referencing student demographic or contact fields. If your district uses SIEM tooling, build a detection rule correlating Canvas API activity volume spikes against known integration baselines. No specific hashes, IPs, or domains are available for IOC-based blocking at this time.

Framework Mappings

MITRE-ATTACK

- **T1530** — Data from Cloud Storage
- **T1078** — Valid Accounts

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

OWASP-TOP10-2021

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

HIPAA-SECURITY

- **164.312(a)(1)** — Access Control
- **164.308(a)(6)(ii)** — Response and Reporting

SOC2-TSC

- **CC7.4** — Responds to identified security incidents

ISO-27001-2022

- **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
T1530	Data from Cloud Storage	Collection
T1078	Valid Accounts	Defense-Evasion

Sources

Source	URL	Tier
	https://www.fox9.com/news/canvas-data-breach-hackers-claim-info-275...	T3
Canvas data breach: Wayzata Public Schools sends warning letter ...	https://www.yahoo.com/news/articles/canvas-data-breach-wayzata-publ...	T3
Fox - Families in Wayzata are being warned about a data breach ...	https://www.facebook.com/fox9kmsp/photos/families-in-wayzata-are-be...	T3
Families in Wayzata are being warned about a data breach ...	https://x.com/FOX9/status/2051478263902400708	T3
Families in Wayzata are being warned about a data breach ...	https://www.facebook.com/fox9kmsp/posts/families-in-wayzata-are-bei...	T3

Organizations should conduct their own validation and consult qualified security professionals before taking action based on this report. Tech Jacks Solutions is not liable for any damages resulting from the use of this information.

Generated 2026-05-05 08:36 UTC by TJS Security Command Center