INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-05-11 05:54 UTC

Canvas system back after cybersecurity breach impacts U of M, colleges across the country

DATA BREACH | HIGH

SCC Item ID	SCC-DBR-2026-0120
Type	Data Breach
Severity	HIGH
Affected Products	Canvas LMS (Instructure), cloud-hosted platform serving U.S. universities including University of Minnesota, University of St. Thomas, Columbia University, and others
Published	3 days ago
Discovery Source	Serper

Executive Summary

A cyberattack against Instructure, the company that operates the Canvas learning management system, disrupted access for thousands of U.S. colleges and universities, including the University of Minnesota, University of St. Thomas, and Columbia University. The attack involved a data breach component; Canvas has been restored, but Instructure has not publicly disclosed the full scope of data accessed or exfiltrated. Organizations dependent on Canvas for academic operations face unquantified data exposure risk until Instructure provides a complete disclosure.

Technical Analysis

A cyberattack against Instructure's cloud-hosted Canvas LMS caused a service outage and reportedly involved unauthorized data access. Star Tribune reporting attributes the attack to ShinyHunters, a financially motivated threat actor known for large-scale data theft from cloud-hosted SaaS platforms; this attribution has not been confirmed by Instructure or a U.S. government authority as of available reporting. MITRE ATT&CK techniques T1190 (Exploit Public-Facing Application), T1657 (Financial Theft), and T1486 (Data Encrypted for Impact) are mapped based on ShinyHunters' historical attack patterns and are speculative; the actual attack sequence has not been disclosed in open sources. No CVE has been assigned. No CWE identifiers are confirmed. CVSS and EPSS scores are not applicable given the absence of a disclosed vulnerability. Patch status, affected versions, and confirmed data types exfiltrated remain unverified. This is a developing situation; technical details are incomplete as of 2026-03-04.

Action Checklist

1. Step 1: Containment, Confirm your institution's Canvas tenant is operating on the restored, post-incident infrastructure. Contact your Instructure account representative or customer support immediately to request a written statement on whether your tenant's data was within the breach scope. Do not wait for a public announcement.
2. Step 2: Detection, Review identity provider (IdP) logs for anomalous Canvas SSO authentication events, particularly any access from unexpected geolocations, IP ranges, or service accounts during the incident window. Pull Canvas API access logs if available through your admin console and look for bulk data export activity or unusual API call volumes. Cross-reference with your SIEM for any outbound data transfers to unknown destinations originating from Canvas-integrated systems.
3. Step 3: Eradication, No patch or vulnerable component has been publicly identified. Institutional response focuses on containment, credential rotation, and detection monitoring rather than software patching. Instruct Instructure to confirm what remediation steps they have applied on the platform side. Rotate any API keys, OAuth tokens, or service account credentials used to integrate Canvas with institutional systems (SIS, SSO, LTI tools). Audit third-party LTI integrations connected to your Canvas instance and disable any that are non-essential.
4. Step 4: Recovery, Verify Canvas administrative access is restricted to authorized accounts only. Confirm your institution's IdP is enforcing MFA for all Canvas-connected accounts. Monitor Canvas audit logs and user activity reports for at least 30 days post-incident. Validate that data feeds between Canvas and your Student Information System (SIS) are intact and have not been tampered with.
5. Step 5: Post-Incident, This incident exposes reliance on a single vendor SaaS platform for critical academic operations without adequate data breach notification SLAs. Review your Instructure contract for breach notification requirements and escalate if SLA timelines were not met. Evaluate whether sensitive student data (PII, academic records) stored in Canvas is minimized per data governance policy. Map Canvas data flows against your FERPA data inventory and update your third-party risk register to reflect elevated risk for this vendor.

IR / Forensic Enrichment

Triage Priority	URGENT
Escalation Criteria	Escalate immediately to institutional legal counsel and the FERPA compliance officer if Instructure confirms your tenant's student PII (names, email addresses, course enrollment, grades, or any FERPA-protected education record) was within the breach scope, or if Instructure fails to provide written confirmation of breach scope within 24 hours of your formal written request — either condition triggers FERPA breach notification analysis and potential state data breach law obligations.
Recovery Notes	Before resuming full Canvas operations, verify with Instructure in writing that your tenant is running on post-incident infrastructure with confirmed remediation applied on the platform side — do not accept verbal assurance. Monitor Canvas API access logs, IdP SSO logs for Canvas, and SIS import history daily for the first two weeks and weekly for 30 days total post-incident, specifically watching for any API calls using tokens that were active during the breach window but were not caught in the Step 3 rotation. Validate SIS data integrity by comparing student enrollment counts and grade record checksums weekly against your SIS source of truth for at least one full academic term, as data tampering in Canvas could affect grade records with downstream academic integrity implications.

Forensic Artifacts	Canvas Admin API access logs (exported from Admin > Logging in Canvas admin console) — specifically calls to bulk data endpoints `/api/v1/accounts/*/users`, `/api/v1/courses/*/enrollments`, and `/api/v1/users/*/profile` during the incident window, which would indicate exfiltration of student roster and PII data | IdP SAML/OIDC transaction logs for Canvas service provider entity ID — specifically authentication events with unexpected source IPs, geolocations outside your institution's normal patterns, or service account principals that do not correspond to human users, which would indicate credential abuse during or after the breach | Canvas SIS Import history (Admin > SIS Imports in admin console) — records of any SIS imports not initiated by your institution's scheduled integration job, which would indicate unauthorized modification of student enrollment, course, or grade data | Network flow records (firewall or proxy logs) from systems hosting Canvas LTI integrations and SIS connector services — specifically outbound HTTPS connections to IP ranges outside Instructure's documented infrastructure during the incident window, indicating potential data exfiltration through integration points | Instructure support ticket and email correspondence log with timestamps — documents the breach notification timeline against your DPA/contractual SLA and establishes the evidentiary record for FERPA compliance analysis and any regulatory notification obligations

Per-Action IR Details

Step 1: Containment — Confirm your institution's Canvas tenant is operating on the restored, post-incident infrastructure. Contact your Instructure account representative or customer support immediately to request a written statement on whether your tenant's data was within the breach scope. Do not wait for a public announcement.

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 — Containment Strategy: isolate affected scope, obtain vendor confirmation of remediation status before resuming normal operations on restored infrastructure

Controls: NIST IR-4 (Incident Handling) — implement containment actions consistent with the incident response plan, NIST IR-6 (Incident Reporting) — require personnel to report suspected incidents and obtain written vendor confirmation of breach scope, NIST SI-5 (Security Alerts, Advisories, and Directives) — receive and act on security advisories from Instructure as an external organization, CIS 7.1 (Establish and Maintain a Vulnerability Management Process) — document vendor remediation status as part of the risk-based response record

Compensating: If your institution lacks a dedicated vendor liaison process, designate one person to email and call your Instructure CSM or support line (support.instructure.com) and log every communication with timestamp in a shared incident log (Google Doc or shared drive folder). Draft a written request citing your institution name, tenant ID (visible in your Canvas admin console under Account > Settings > Account ID), and ask specifically: (1) Was our tenant's data accessed or exfiltrated? (2) What infrastructure changes were made during restoration? (3) What is your breach notification timeline? Save all responses as PDF.

Evidence: Before contacting Instructure, capture a timestamped screenshot of your Canvas admin console showing current system status and tenant ID. Pull your institution's Canvas uptime and availability logs from your IT monitoring tool (or Instructure's status page at status.instructure.com) for the incident window to document the outage period. Preserve any automated alert emails received from Instructure during the incident window — these establish your notification timeline for potential FERPA breach reporting obligations.

Step 2: Detection — Review identity provider (IdP) logs for anomalous Canvas SSO authentication events, particularly any access from unexpected geolocations, IP ranges, or service accounts during the incident window. Pull Canvas API access logs if available through your admin console and look for bulk data export activity or unusual API call volumes. Cross-reference with your SIEM for any outbound data transfers to unknown destinations originating from Canvas-integrated systems.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis: correlate log data from multiple sources, prioritize analysis on authentication events and data access patterns during the confirmed incident window

Controls: NIST AU-2 (Event Logging) — ensure IdP and Canvas API access events are captured in audit logs, NIST AU-6 (Audit Record Review, Analysis, and Reporting) — review and analyze system audit records for anomalous Canvas SSO and API activity, NIST AU-12 (Audit Record Generation) — verify that Canvas-integrated systems (IdP, SIS) are generating complete audit records for the incident window, NIST SI-4 (System Monitoring) — monitor for anomalous outbound data transfers from Canvas-integrated systems, CIS 8.2 (Collect Audit Logs) — ensure logging has been enabled across Canvas-integrated enterprise assets including IdP and SIS connectors

Compensating: Without a SIEM, query your IdP directly: For Azure AD/Entra ID, run `Get-MgAuditLogSignIn -Filter "appDisplayName eq 'Canvas' and createdDateTime ge 2025-01-01"` (adjust date to incident window start) and export to CSV; filter for ResultType != 0 (failed) and unfamiliar IP ranges. For Shibboleth/SAML, parse `/var/log/shibboleth/transaction.log` for Canvas entityID entries with unexpected source IPs. For Canvas API logs, navigate to Admin > Logging in your Canvas admin console and export API access logs; use `grep` or Excel to filter for calls to `/api/v1/accounts/*/users` (bulk user export) or `/api/v1/courses/*/enrollments` (enrollment data export) with anomalous OAuth token IDs. Use `zeek` or Wireshark packet captures on your SIS integration host to identify unexpected outbound connections to non-Instructure IP ranges.

Evidence: Preserve IdP authentication logs for the full incident window plus 72 hours before and after, specifically SAML assertion logs showing Canvas service provider entity ID, source IP, and authenticated user UPN. Export Canvas API access logs from the admin console before they age out — Instructure's default retention may be 30 days or less. Capture network flow data (NetFlow or firewall logs) from systems hosting Canvas LTI integrations and SIS connectors, specifically looking for outbound HTTPS connections to IP ranges outside Instructure's documented infrastructure (AS19488, instructure.com subdomains). Document all OAuth token IDs and API keys that had active sessions during the incident window.

Step 3: Eradication — No patch is available because no CVE or specific vulnerability has been disclosed. Instruct Instructure to confirm what remediation steps they have applied on the platform side. Rotate any API keys, OAuth tokens, or service account credentials used to integrate Canvas with institutional systems (SIS, SSO, LTI tools). Audit third-party LTI integrations connected to your Canvas instance and disable any that are non-essential.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication: remove malicious artifacts, rotate compromised credentials, and verify the threat has been eliminated from the environment before recovery proceeds

Controls: NIST IR-4 (Incident Handling) — eradication actions are a required component of the incident handling capability, NIST SI-2 (Flaw Remediation) — identify and correct system flaws; obtain vendor confirmation of platform-side remediation since no CVE patch is institutionally applicable, NIST SI-7 (Software, Firmware, and Information Integrity) — verify integrity of Canvas LTI integrations and SIS data connector configurations post-incident, NIST AC-2 (Account Management) — rotate and audit service accounts and API credentials used by Canvas integrations, CIS 5.1 (Establish and Maintain an Inventory of Accounts) — audit all service accounts and API tokens connected to Canvas before rotating

Compensating: Document all Canvas API keys by navigating to Admin > Developer Keys in your Canvas admin console — screenshot the full list with token names, creation dates, and last-used dates before revoking. Revoke all keys created before the incident and reissue only what is actively needed. For LTI integrations, go to Admin > Settings > Apps and export the list; cross-reference against your software inventory (CIS 2.1) and disable any LTI tool with no documented owner or last used more than 90 days ago. For SSO service accounts in your IdP, run `Get-ADServiceAccount -Filter *` (AD) or equivalent LDAP query and disable any account whose description references Canvas or Instructure that is not actively managed. Log every credential rotation with timestamp and responsible party in your incident record.

Evidence: Before revoking credentials, capture the full Canvas Developer Keys list as a timestamped export — this documents which tokens were active during the breach and may be needed for FERPA breach notification or legal hold. Export your LTI integration list from the Canvas admin console, noting each tool's redirect URI and OAuth consumer key. If any LTI tools use externally hosted endpoints (non-institutional domains), flag those endpoints for threat intelligence lookup. Preserve IdP service account last-logon timestamps before any account modifications are

made.

Step 4: Recovery — Verify Canvas administrative access is restricted to authorized accounts only. Confirm your institution's IdP is enforcing MFA for all Canvas-connected accounts. Monitor Canvas audit logs and user activity reports for at least 30 days post-incident. Validate that data feeds between Canvas and your Student Information System (SIS) are intact and have not been tampered with.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery: restore systems to normal operation with verified integrity, confirm security controls are functioning, and establish enhanced monitoring for the post-incident period

Controls: NIST IR-4 (Incident Handling) — recovery actions must be consistent with the incident response plan and include verification of restored security posture, NIST SI-7 (Software, Firmware, and Information Integrity) — verify integrity of SIS data feeds and Canvas configuration against known-good baselines, NIST IA-5 (Authenticator Management) — enforce MFA for all Canvas-connected accounts through IdP policy, NIST AU-6 (Audit Record Review, Analysis, and Reporting) — sustain enhanced audit log review for 30 days post-incident to detect any persistent access, CIS 6.3 (Require MFA for Externally-Exposed Applications) — enforce MFA for Canvas as an externally-exposed application accessed via IdP, CIS 6.5 (Require MFA for Administrative Access) — enforce MFA specifically for Canvas admin role accounts

Compensating: To verify admin account restriction without an IAM tool, export your Canvas admin role list via API: `curl -H 'Authorization: Bearer ' 'https://.instructure.com/api/v1/accounts/1/admins'` and compare against your authorized admin roster in writing. For MFA enforcement, verify your IdP Conditional Access policy (Azure AD) or authentication context (Okta) requires MFA for the Canvas application specifically — test with a non-MFA account to confirm enforcement. For SIS feed integrity, compare row counts and checksums of the most recent SIS import file against the previous week's import using `md5sum` or `sha256sum` on the CSV files your SIS exports; flag any unexpected record deletions or field changes. Set a calendar reminder to review Canvas User Activity reports weekly for 30 days — export from Admin > Reports > Last User Access.

Evidence: Before declaring recovery complete, capture a baseline export of all Canvas admin role assignments (as above) and store it as the verified clean-state reference. Document the exact timestamp when MFA enforcement was confirmed active in your IdP for Canvas. Pull a Canvas SIS import history report (Admin > SIS Imports) for the incident window and 30 days prior — look for any imports not initiated by your institution's scheduled integration, which could indicate unauthorized data manipulation. Preserve this export as a forensic artifact.

Step 5: Post-Incident — This incident exposes reliance on a single vendor SaaS platform for critical academic operations without adequate data breach notification SLAs. Review your Instructure contract for breach notification requirements and escalate if SLA timelines were not met. Evaluate whether sensitive student data (PII, academic records) stored in Canvas is minimized per data governance policy. Map Canvas data flows against your FERPA data inventory and update your third-party risk register to reflect elevated risk for this vendor.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity: conduct lessons-learned review, update policies and controls, share intelligence, and identify process improvements to prevent recurrence

Controls: NIST IR-4 (Incident Handling) — post-incident activity is a required phase; update the incident handling capability based on lessons learned, NIST IR-8 (Incident Response Plan) — update the incident response plan to address gaps exposed by this vendor-side breach, including SaaS provider notification SLA requirements, NIST SI-12 (Information Management and Retention) — manage and retain information within Canvas in accordance with applicable laws including FERPA; minimize PII stored in Canvas to what is operationally necessary, NIST RA-3 (Risk Assessment) — update the risk assessment for Instructure/Canvas to reflect the elevated third-party risk demonstrated by this incident, CIS 3.2 (Establish and Maintain a Data Inventory) — update the data inventory to reflect all sensitive data (student PII, academic records, grades) stored in or transiting Canvas, CIS 7.1 (Establish and Maintain a Vulnerability Management Process) — incorporate vendor-side breach events into the vulnerability and risk management process for SaaS dependencies

Compensating: Without a formal third-party risk management platform, create or update a vendor risk register entry for Instructure in a spreadsheet that documents: (1) data categories stored in Canvas (student PII, grades, course submissions — all FERPA-protected), (2) contractual breach notification SLA (extract the exact clause and hours from your DPA/BAA with Instructure), (3) actual notification timeline from this incident vs. contracted SLA, and (4) risk rating change. For FERPA data flow mapping, use your SIS integration documentation to list every field transmitted to Canvas via SIS import and flag any fields that are not required for LMS functionality (e.g., SSN, date of birth, financial aid status). Submit a formal data minimization request to your Instructure account rep to delete non-essential fields from Canvas data stores. File the lessons-learned report using your institution's standard IR documentation template and retain per NIST AU-11 (Audit Record Retention) requirements.

Evidence: Preserve your Instructure Data Processing Agreement (DPA) and any BAA as legal hold documents — the breach notification clause is the evidentiary basis for any SLA violation claim. Document the timestamp of Instructure's first public disclosure and first direct customer notification to your institution; compare against the contractual SLA window. Retain all incident correspondence with Instructure (emails, support tickets, written statements obtained in Step 1) as part of the post-incident record. If your institution is subject to state data breach notification laws (e.g., Minnesota Statute §325E.61 or New York Education Law §2-d for Columbia), document the timeline analysis that determines whether student PII exposure triggers mandatory notification obligations.

Detection Guidance

No confirmed IOCs are available in open sources as of 2026-03-04. Detection should focus on behavioral indicators. Review IdP and SSO logs for Canvas authentication anomalies during the incident window, including failed logins at high volume, logins from unexpected IP ranges or countries, and service account activity outside normal hours. In your SIEM, query for Canvas-originating API calls with high request volumes, bulk record access patterns, or calls to data export endpoints. If your institution uses a CASB, pull Canvas activity reports for data exfiltration indicators such as large downloads or unusual file transfers. Monitor student and faculty account activity for signs of credential-based access by unauthorized parties. ShinyHunters has historically leveraged stolen credentials and cloud misconfigurations; audit Canvas admin accounts for password reuse and ensure MFA is enforced. Attribution to ShinyHunters is medium-confidence per Star Tribune reporting only; treat IOC hunting as speculative until Instructure or a government authority provides confirmed indicators.

Framework Mappings

MITRE-ATTACK

- **T1190** — Exploit Public-Facing Application
- **T1657** — Financial Theft
- **T1486** — Data Encrypted for Impact

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
- **CP-9** — System Backup
- **CP-10** — System Recovery and Reconstitution

ISO-27001-2022

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

HIPAA-SECURITY

- **164.308(a)(6)(ii)** — Response and Reporting

SOC2-TSC

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

NIST-CSF-2

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

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1190	Exploit Public-Facing Application	Initial-Access
T1657	Financial Theft	Impact
T1486	Data Encrypted for Impact	Impact

Sources

Source	URL	Tier
	https://kstp.com/kstp-news/top-news/cybersecurity-breach-impacting-...	T3
Canvas back online for most after data breach; Columbia University ...	https://www.aol.com/news/canvas-back-online-most-data-103133065.html	T3
U of M & St. Thomas among colleges affected by cyberattack	https://www.startribune.com/university-of-minnesota-canvas-outage-d...	T3
Canvas system back online after cyberattack disrupted thousands of ...	https://www.fox2detroit.com/news/canvas-system-back-online-cyberatt...	T3
Canvas system is online after a cyberattack disrupted thousands of ...	https://www.sooleader.com/michigan-news-ap/canvas-system-is-online-...	T3

DISCLAIMER

Generated 2026-05-11 05:54 UTC by TJS Security Command Center