INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-05-09 06:26 UTC

Ransomware Attack on Instructure Canvas Disrupts College Final Exams Nationwide

DATA BREACH | HIGH

SCC Item ID	SCC-DBR-2026-0118
Type	Data Breach
Severity	HIGH
Affected Products	Instructure Canvas LMS (cloud-hosted platform, specific version not publicly disclosed)
Published	15 hours ago
Discovery Source	Serper

Executive Summary

A ransomware group attacked Instructure's Canvas learning management system on or around May 8, 2026, causing a service outage that disrupted final exams at colleges and universities nationwide. The incident involved a confirmed data breach, prompting institutional warnings against logging back in even after service restoration. Organizations relying on Canvas as a SaaS provider face third-party supply chain risk with no direct patch action available to them; exposure is entirely dependent on Instructure's remediation and transparency.

Technical Analysis

This incident is a ransomware intrusion against Instructure's cloud-hosted Canvas LMS, a SaaS platform. No CVE has been assigned; this is not a discrete disclosed vulnerability but an intrusion and ransomware deployment against a SaaS provider's infrastructure. MITRE ATT&CK techniques observed or inferred: T1078 (Valid Accounts, likely initial access vector), T1190 (Exploit Public-Facing Application, possible secondary vector), T1657 (Financial Extortion, ransomware demand), T1486 (Data Encrypted for Impact, ransomware payload). No specific Canvas version is publicly implicated; the attack targeted Instructure's hosted environment, not customer-managed deployments. No patch is available to end-user institutions; remediation is Instructure's responsibility. Attribution to a named threat actor group remains unconfirmed as of available reporting. Data breach scope has not been formally disclosed by Instructure. Source quality is T3 (news media, no vendor advisory or CISA alert confirmed at time of data).

Action Checklist

1. Containment: If your institution uses Canvas, treat Canvas credentials as potentially compromised. Suspend Canvas SSO integrations with your IdP until Instructure confirms breach scope. Do not re-enable Canvas access for users until Instructure issues a formal incident advisory.
2. Detection: Audit IdP and SSO logs for anomalous Canvas-originated authentication events in the window of April 2026 to present. Review any data feeds or API integrations your institution has with Canvas for unexpected outbound connections or data exfiltration indicators. Check SIEM for authentication events tied to Canvas service accounts.
3. Eradication: Reset all service account credentials used for Canvas API integrations. Force password resets for any accounts where Canvas credentials may have been reused across institutional systems. Rotate API keys and OAuth tokens issued to Canvas.
4. Recovery: Before restoring full Canvas access, obtain a written incident summary from Instructure specifying breach scope, affected data types, and remediation steps taken. Validate that SSO and API integrations behave as expected post-reconnection. Monitor for unauthorized access attempts using reset credentials.
5. Post-Incident: Review your institution's third-party SaaS risk assessment process. Canvas represents a high-dependency, low-visibility SaaS supply chain risk. Confirm your vendor contracts include breach notification SLAs. Evaluate whether critical academic operations (exam administration, grade submission) have manual fallback procedures.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate to institutional legal counsel and privacy officer immediately if Instructure's written breach advisory confirms that FERPA-covered student education records (grades, enrollment, advising records, financial aid data) were accessed or exfiltrated, triggering institutional breach notification obligations under FERPA and applicable state data breach notification statutes.
Recovery Notes	Do not restore Canvas SSO or API integrations until Instructure issues a formal written incident advisory confirming the scope of compromise and remediation actions taken on their infrastructure — verbal or informal communications are insufficient given FERPA and contractual obligations. Post-restoration, maintain heightened monitoring of Canvas admin audit logs, authentication events, and SIS integration API call volumes for a minimum of 30 days, with daily analyst review for the first 72 hours. Any anomalous Canvas admin actions (unexpected enrollment changes, grade modifications, new admin accounts) observed post-restoration should be treated as indicators of persistent access and trigger re-containment.

Forensic Artifacts	IdP audit logs (Azure AD Sign-in logs, Okta System Log, Shibboleth audit.log) filtered for Canvas SAML assertions and OAuth token grants from April 1, 2026 to present — primary evidence for determining whether Canvas-federated credentials were abused to access institutional systems laterally during or after the ransomware event | Canvas Developer Keys and API access token metadata export from Canvas Admin console (Admin > Developer Keys) — establishes which institutional API integrations were active and potentially exposed to the ransomware operator during the breach window, including token scopes and last-used timestamps | Network proxy or firewall egress logs for outbound HTTPS traffic to *.instructure.com and *.canvascdn.com covering April–May 2026 — ransomware operators commonly conduct data exfiltration before encryption; anomalous upload volume spikes to Canvas infrastructure or to unknown IPs during this window indicate potential pre-encryption data theft | Canvas Data 2 pipeline job logs or Canvas Data export records if your institution uses automated bulk data exports — unauthorized or duplicated bulk export jobs initiated during the April–May 2026 window would indicate threat actor access to student PII at scale via Instructure's own data pipeline infrastructure | Student Information System (Banner, Workday Student, PeopleSoft) integration service account authentication logs for credentials used in Canvas API calls — any authentications from unexpected source IPs or outside scheduled sync windows during April–May 2026 indicate potential credential abuse by the ransomware operator using keys harvested from Instructure's compromised environment

Per-Action IR Details

Containment — If your institution uses Canvas, treat Canvas credentials as potentially compromised. Suspend Canvas SSO integrations with your IdP until Instructure confirms breach scope. Do not re-enable Canvas access for users until Instructure issues a formal incident advisory.

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 — Containment Strategy; RS.MA-01 — Incident response plan execution with third-party coordination

Controls: NIST IR-4 (Incident Handling), NIST AC-17 (Remote Access) — suspend remote/federated access paths until provider confirms scope, NIST SC-7 (Boundary Protection) — isolate Canvas SSO trust relationship at IdP boundary, CIS 6.2 (Establish an Access Revoking Process) — revoke SSO delegation to Canvas as an untrusted external application, CIS 6.3 (Require MFA for Externally-Exposed Applications) — MFA enforcement gap exposed when SSO trust is extended to a compromised SaaS provider

Compensating: For teams without enterprise IdP tooling: disable the Canvas SAML or OIDC application registration directly in your identity provider admin console (Azure AD, Okta, Google Workspace, Shibboleth) rather than waiting for automated policy. In Shibboleth or SimpleSAMLphp environments, comment out the Canvas SP metadata entry and restart the IdP service. Block Canvas OAuth callback URIs at the perimeter firewall using an outbound ACL rule targeting `*.instructure.com` and `*.canvascdn.com`. Document the timestamp of suspension for breach notification recordkeeping.

Evidence: Before suspending SSO, export and preserve IdP audit logs showing all Canvas-originated SAML assertions and OAuth token grants for the window of April 1, 2026 to present. In Azure AD: export Sign-in logs filtered by Application = 'Canvas' and flag any logins from anomalous geographies or outside business hours. In Okta: export System Log events for `app.oauth2.token.grant` and `user.authentication.sso` where target app matches Canvas. Capture current Canvas API token inventory from your LMS admin panel before rotating — this establishes baseline of what was active during the breach window.

Detection — Audit IdP and SSO logs for anomalous Canvas-originated authentication events in the window of April 2026 to present. Review any data feeds or API integrations your institution has with Canvas for unexpected outbound connections or data exfiltration indicators. Check SIEM for authentication events tied to Canvas service accounts.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis; DE.AE-03 — Information correlated from multiple sources; DE.CM-06 — External service provider activities monitored

Controls: NIST AU-6 (Audit Record Review, Analysis, and Reporting) — review IdP logs for anomalous Canvas authentication patterns, NIST SI-4 (System Monitoring) — monitor for unauthorized data flows originating from Canvas API integration accounts, NIST IR-5 (Incident Monitoring) — track and document all Canvas-related authentication anomalies as incident evidence, CIS 8.2 (Collect Audit Logs) — ensure IdP, SIS integration, and network egress logs are collected and retained covering April 2026 to present

Compensating: Without SIEM: query Azure AD Sign-in logs directly via Microsoft Graph API using PowerShell — `Get-MgAuditLogSignIn -Filter "appDisplayName eq 'Canvas' and createdDateTime ge 2026-04-01" | Export-Csv canvas_signins.csv`. For Okta without SIEM: use the Okta System Log API with query `filter=target.displayName+eq+'Canvas'&since=2026-04-01T00:00:00Z`. For network egress review without NDR tooling: use Wireshark or tcpdump on the integration server to capture traffic to Canvas API endpoints (`*.instructure.com` on port 443) and inspect for anomalous data volumes or off-hours transfer patterns. For SIS/Banner integrations: diff current Canvas enrollment API call logs against baseline volume — unexpected bulk data pulls (student PII, grades) are a key exfiltration indicator.

Evidence: Collect: (1) IdP sign-in logs for all Canvas SSO events April 1–present, flagging any service account authentications outside scheduled sync windows. (2) Network flow logs or proxy logs showing outbound HTTPS volume to `*.instructure.com` — ransomware operators commonly exfiltrate data prior to encryption, so anomalous upload spikes to Canvas infrastructure or to unknown IPs masquerading as Canvas endpoints are significant. (3) Canvas Data 2 or Canvas Data pipeline job logs if your institution uses automated data exports — check for unauthorized or duplicated export jobs initiated during the April–May 2026 window. (4) Student Information System (Banner, Workday Student, PeopleSoft) integration service account authentication logs for Canvas API credentials.

Eradication — Reset all service account credentials used for Canvas API integrations. Force password resets for any accounts where Canvas credentials may have been reused across institutional systems. Rotate API keys and OAuth tokens issued to Canvas.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication; RS.MA-01 — Execute containment and mitigation actions

Controls: NIST IA-5 (Authenticator Management) — rotate all Canvas API keys, OAuth tokens, and service account passwords issued prior to breach confirmation, NIST AC-2 (Account Management) — audit and reset all service accounts whose credentials were scoped to Canvas integrations, NIST SI-2 (Flaw Remediation) — treat credential exposure from a confirmed third-party breach as a flaw requiring immediate remediation, CIS 5.2 (Use Unique Passwords) — identify any credential reuse across Canvas and institutional systems (SIS, email, VPN) and force reset on all reused credentials, CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts) — verify Canvas admin-level API tokens were not issued to shared or general-purpose accounts

Compensating: Without PAM tooling: generate a full inventory of Canvas Developer Keys and API tokens from the Canvas Admin console (Settings > Developer Keys) and revoke all tokens issued before the breach notification date. Script token revocation via Canvas API: `curl -X DELETE https://.instructure.com/api/v1/accounts/self/developer_keys/ -H 'Authorization: Bearer '`. For credential reuse identification without enterprise tooling: extract Canvas-registered email addresses from your IdP and cross-reference against accounts with identical passwords using a local Have I Been Pwned (HIBP) Enterprise API query or by running a controlled credential audit using a script against your LDAP/AD directory. Force AD password resets for affected accounts via PowerShell: `Set-ADUser -Identity -ChangePasswordAtLogon $true`.

Evidence: Before rotating credentials, preserve: (1) Full export of all Canvas Developer Keys and associated access token metadata (creation date, last used date, scopes) from Canvas Admin console — this establishes which tokens were active and potentially exposed. (2) Active OAuth grant list from your IdP showing which institutional applications were granted Canvas OAuth scopes. (3) Service account last-login timestamps from AD or LDAP for all accounts used in Canvas integrations — any logins from unexpected IPs or outside maintenance windows during April–May 2026 indicate potential credential abuse by the ransomware operator prior to encryption.

Recovery — Before restoring full Canvas access, obtain a written incident summary from Instructure specifying breach scope, affected data types, and remediation steps taken. Validate that SSO and API

integrations behave as expected post-reconnection. Monitor for unauthorized access attempts using reset credentials.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery; RS.MA-01 — Execute recovery plan and verify integrity before restoration

Controls: NIST IR-4 (Incident Handling) — recovery actions must be coordinated with Instructure's formal incident advisory before re-enabling institutional access, NIST CA-7 (Continuous Monitoring) — establish heightened monitoring of Canvas SSO and API integration behavior for minimum 30 days post-restoration, NIST AU-6 (Audit Record Review, Analysis, and Reporting) — review authentication and API access logs during the first 72 hours post-reconnection for anomalous patterns, CIS 6.3 (Require MFA for Externally-Exposed Applications) — enforce MFA on all Canvas user accounts before restoring SSO, with particular attention to admin and instructor roles

Compensating: Without enterprise monitoring tooling: implement a manual 72-hour observation window post-reconnection during which an analyst reviews Canvas admin audit logs daily (Admin > Logging in Canvas) for unexpected admin actions, enrollment changes, or grade modifications. Set up free alerting using a scheduled PowerShell or bash script that queries the Canvas API for admin-level events (`GET /api/v1/audit/grade_change/courses` and `GET /api/v1/audit/authentication`) and pipes results to email if volume exceeds baseline. Use Wireshark on the Canvas integration server for the first 48 hours post-reconnection to capture any unexpected outbound data flows that could indicate re-compromise.

Evidence: Before re-enabling Canvas SSO, obtain and retain: (1) Written attestation from Instructure (email or formal advisory) confirming breach scope, affected data categories (FERPA-covered student records, PII, financial aid data), and the specific remediation actions taken on their infrastructure — this is required for your institution's breach notification assessment. (2) Baseline snapshot of Canvas admin audit log entries (enrollment counts, grade records, admin user list) immediately prior to reconnection to enable diff comparison during the monitoring window. (3) Network baseline of expected API call volume and cadence from your SIS integration to Canvas for anomaly comparison post-restoration.

Post-Incident — Review your institution's third-party SaaS risk assessment process. Canvas represents a high-dependency, low-visibility SaaS supply chain risk. Confirm your vendor contracts include breach notification SLAs. Evaluate whether critical academic operations (exam administration, grade submission) have manual fallback procedures.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity; DE.AE-07 — Cyber threat intelligence integrated into adverse event analysis to improve detection and organizational risk posture

Controls: NIST IR-8 (Incident Response Plan) — update IR plan to include SaaS provider outage and third-party breach scenarios, specifically naming Canvas and equivalent high-dependency academic platforms, NIST RA-3 (Risk Assessment) — re-evaluate residual risk of Canvas dependency given confirmed ransomware impact on exam administration and potential FERPA data exposure, NIST SA-9 (External System Services) — enforce contract requirements for breach notification timelines, incident reporting obligations, and right-to-audit clauses with Instructure, NIST CP-2 (Contingency Plan) — develop and test manual fallback procedures for exam administration and grade submission that do not depend on Canvas availability, CIS 7.1 (Establish and Maintain a Vulnerability Management Process) — extend vulnerability and risk management scope to include SaaS provider breach monitoring as a standing process, CIS 3.2 (Establish and Maintain a Data Inventory) — inventory all student PII, FERPA-covered records, and institutional data stored in or transmitted through Canvas to support breach notification scope assessment

Compensating: Without a formal vendor risk management program: create a one-page SaaS dependency register (spreadsheet) listing Canvas alongside other high-dependency platforms (Microsoft 365, Zoom, Banner), documenting data types stored, breach notification contact, current contract SLA, and manual fallback procedure status. Review your Instructure Master Services Agreement and Data Processing Addendum specifically for FERPA breach notification timelines — FERPA requires notification to affected students when education records are compromised. If contracts lack notification SLAs, initiate a formal amendment request citing this incident. Draft a one-page manual exam administration procedure (paper-based or email-submitted) that department chairs can activate within two hours of a future Canvas outage.

Evidence: Preserve for lessons-learned and potential regulatory review: (1) Timeline documentation of when your institution first learned of the Canvas outage, when Instructure issued any communications, and when your institution took each containment action — this establishes your FERPA breach notification clock. (2) Inventory of FERPA-covered data categories processed through Canvas (grades, enrollment records, financial aid references, advising notes) to determine whether a FERPA breach notification obligation exists. (3) Records of any exam disruptions, student PII exposure, or operational harm caused by the outage for inclusion in the post-incident report and future vendor contract negotiations.

Detection Guidance

No confirmed IOCs are publicly available at this time. Detection should focus on lateral indicators: review IdP logs for Canvas-sourced authentication anomalies; audit API gateway logs for unexpected Canvas service account activity; search SIEM for outbound data transfers to unfamiliar destinations during the April-May 2026 window. If your institution uses Canvas Data (the analytics pipeline), treat that data export as potentially compromised and audit downstream systems that ingest it. Monitor for credential stuffing attempts against institutional accounts using email addresses known to be in Canvas; attackers may leverage breached Canvas credentials against other services.

Framework Mappings

MITRE-ATTACK

- **T1078** — Valid Accounts
- **T1190** — Exploit Public-Facing Application
- **T1657** — Financial Theft
- **T1486** — Data Encrypted for Impact

NIST-800-53R5

- **AC-2** — Account Management
- **AC-6** — Least Privilege
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **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
- **IR-4** — Incident Handling

NIST-CSF-2

- **RS.MI-01** — Incidents are contained
- **RS.CO-03** — Recovery activities and progress communicated

HIPAA-SECURITY

- **164.308(a)(7)(ii)(A)** — Data Backup Plan
- **164.308(a)(6)(ii)** — Response and Reporting

ISO-27001-2022

- **A.5.29** — Information security during disruption
- **A.8.8** — Management of technical vulnerabilities
- **A.5.34** — Privacy and protection of personal information
- **A.5.23** — Information security for use of cloud services

SOC2-TSC

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

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1078	Valid Accounts	Defense-Evasion
T1190	Exploit Public-Facing Application	Initial-Access
T1657	Financial Theft	Impact
T1486	Data Encrypted for Impact	Impact

Sources

Source	URL	Tier
	https://www.npr.org/2026/05/08/nx-s1-5815956/canvas-data-breach-sch...	T3
Canvas back online after cyberattack while many colleges having ...	https://www.youtube.com/watch?v=6hBzEC4HOFQ	T3
A Canvas Outage Tied to a Cyberattack Has Wreaked Havoc on ...	https://www.usnews.com/news/us/articles/2026-05-08/a-canvas-outage-...	T3
Canvas back online, but FIU & Broward schools wait to ... - YouTube	https://www.youtube.com/watch?v=hwx5gshK7Uo	T3
Schools and universities across the country are recovering from an ...	https://www.facebook.com/wbalradio/posts/schools-and-universities-a...	T3

DISCLAIMER

This intelligence report is produced by Tech Jacks Solutions Security Command Center (SCC) for informational purposes only. It does not constitute professional security advice, legal counsel, or an incident response engagement. The information herein is derived from publicly available sources and AI-assisted analysis; while every effort is made to ensure accuracy, Tech Jacks Solutions makes no warranties regarding completeness or timeliness. 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 2026-05-09 06:26 UTC by TJS Security Command Center