Learning Technology Center

vCISO Program

Monthly Cyber Threat Intelligence Brief

October 2026

Companion to the full October 2026 Monthly Cyber Threat Intelligence report

Covers September 20, 2026 to October 19, 2026

Executive Summary

October's largest K-12 data exposures came through vendors, not district networks. A stolen login at California's testing contractor exposed millions of student records, and a Frontline Education breach exposed staff SSNs in several states. At least 18 US K-12 schools and districts were hit by or listed for cyberattacks (leak-site claims, not publicly confirmed). Jerome, ID closed for two days after attackers reached cameras, locks, and HVAC.

Third-party and identity risk dominate: ConnectWise's Microsoft 365 apps were abused, phishing moved to device codes and calendar invites, and Citrix NetScaler suffered three zero-days with education among victims. AI is now part of real intrusions. Hold vendors accountable, tighten identity controls on people and applications, and patch internet-facing systems on a days-not-weeks timeline.

18
US K-12 schools and districts newly hit or listed on leak sites

10
confirmed by the school or reported by the press

~4 months
A stolen testing-vendor login went undetected (May 22 – Sep 18)

1,413
CVEs fixed in Microsoft's record October Patch Tuesday

Monthly Areas of Focus

Citrix NetScaler – Three Zero-Days Exploited, Education Among Victims

Severity: Critical

What happened: *CVE-2026-88771 and 88772 (CVSS v4 9.5) were exploited before patches existed and added to KEV Sep 27; CVE-2026-88779 followed Oct 4. Mandiant found likely victims including the education sector.*

Recommended action: *Upgrade to 14.1-73.41 or 13.1-64.28, run Citrix's IoC script before upgrading, hunt for web shells, and rotate tokens and credentials. Patching alone does not prove the appliance is clean.*

Frontline Education Breach – Employee and Applicant Data Exposed

Severity: Critical

What happened: *A flaw in an unnamed third-party product exposed employee SSNs and addresses and applicant data; South Carolina districts were told student health data may be involved.*

Recommended action: *Confirm which Frontline modules you use and whether you were notified, request affected counts in writing, review PIPA/SOPPA duties, and require call-back verification for banking changes.*

California State Testing Breach – One Stolen Credential, Millions of Student Records

Severity: High

What happened: *A compromised login on ETS's SFTP site let an attacker copy CAASPP/ELPAC files from May 22 to Sep 18.*

Recommended action: *Ask assessment, SIS, and integration vendors whether SFTP requires MFA or keys, IP restrictions, and logging; clear stale files from district drop folders.*

Microsoft – Record Patch Tuesday, Exploited Windows Shell and SharePoint Flaws

Severity: Critical

What happened: *CVE-2026-96951 bypasses Mark of the Web and was exploited (KEV Oct 13); SharePoint CVE-2026-65660 was exploited in late September.*

Recommended action: *Deploy October updates now, apply June/August SharePoint updates and disable anonymous access, install the Exchange "September 2026 v2" update, and enable ASR rules.*

Remote-Access and Network Infrastructure – Cisco, SonicWall, and Ivanti

Severity: High

What happened: *Cisco SD-WAN Manager CVE-2026-76504 (CVSS 9.8) was exploited; SonicWall SMA 1000 CVE-2026-102255 (CVSS 10.0) saw attempts two days after its patch; Ivanti Connect Secure CVE-2026-104935 joined KEV.*

Recommended action: *Patch to fixed releases, review logs for unknown logins, and put management interfaces on a VPN-only VLAN with MFA.*

ConnectWise Cloud Backup Suspended – Trusted Microsoft 365 Apps Abused

Severity: High

What happened: *Attackers used ConnectWise app identities to sign in to almost 1,000 customer tenants, about 300 successfully; Cloud Backup (formerly SkyKick) is suspended with no restore date.*

Recommended action: *Ask your MSP whether ConnectWise/SkyKick apps are in your tenant, review sign-ins since Oct 13, audit app secrets and admin grants, and arrange alternate backup.*

Phishing Beyond the Inbox – Device Codes, Calendar Invites, and Help Desk Calls

Severity: High

What happened: *The Wazza kit abuses Microsoft device-code sign-in, calendar-invite phishing is growing rapidly, and spoofed help desk calls opened the Astrana Health breach.*

Recommended action: *Block device-code flow via Conditional Access, limit external calendar invites, and give the help desk a call-back verification script.*

Endpoint Defense Evasion – Fake Installers, ChatGPT-Hosted ClickFix, Defender Tampering

Severity: High

What happened: *Fake LastPass installers delivered a driver that kills 145 security products; malicious Custom GPTs pushed ClickFix lures that installed a remote access trojan.*

Recommended action: *Remove local admin, enable the vulnerable driver blocklist and tamper protection, and restrict PowerShell.*

Apple CoreGraphics Zero-Day (CVE-2026-86950)

Severity: High

What happened: *An exploited CoreGraphics flaw (KEV Sep 29) now has a public PDF proof of concept.*

Recommended action: *Require iOS/iPadOS 26.7.1 and macOS 26.7.1 or 15.8.1 through MDM and isolate devices that cannot update.*

Website Platforms – WordPress Core Exploited Within Hours, Critical Drupal Fixes

Severity: High

What happened: *WordPress CVE-2026-87902 was attacked less than five hours after the 7.1.2 fix; Drupal warned that exploits for CVE-2026-108097 could emerge within hours or days.*

Recommended action: *Update WordPress to 7.1.2 and Drupal to 10.6.19, 11.3.19, or 11.4.10.*

AI-Driven Attacks Move From Research to Real Intrusions

Severity: Medium

What happened: *An AI agent ran a live breach of DIVD via Zammad zero-days; Storm-3168 deleted 100+ Azure storage accounts in about seven minutes.*

Recommended action: *Take self-hosted AI tools off the internet, upgrade Zammad to 7, apply Azure delete locks.*

Building and Physical Systems Become Ransomware Targets

Severity: Medium

What happened: *Attackers reached cameras, door locks, and HVAC in Jerome, ID; attacks on exposed refrigeration controllers disrupted about 700 French supermarkets.*

Recommended action: *Inventory and segment building systems, remove internet-facing management; require contractor MFA.*

Old and Overlooked Software – LibreOffice, Legacy KEV Additions, Adobe

Severity: Medium

What happened: *A malicious spreadsheet can run code in LibreOffice and OpenOffice when Java is enabled; CISA added five old ProFTPD, ONLYOFFICE, Strapi, Struts, and BIND flaws to KEV.*

Recommended action: *Update LibreOffice (26.2.5/26.8.0) and OpenOffice (4.1.17); retire legacy servers.*

Law Enforcement Pressure – ShinyHunters, KillSec, and a Fraudulent "Recovery" Firm

Severity: Medium

What happened: *Arrests followed ShinyHunters' FBI portal breach, police dismantled KillSec, and DOJ charged MonsterCloud's owner with secretly paying ransoms.*

Recommended action: *Re-check Canvas and PowerSchool exposure, confirm PeopleSoft patches; pre-select an IR firm.*

Platform Changes and Planning Items

Severity: Low

What happened: *Teams adds custom file-type blocking and Outlook will block MSIX attachments in November.*

Recommended action: *Enable Teams file-type checking now, lock and MFA-protect the district domain registrar.*

Recommendations

Credential Audit

Rotate exposed remote-access credentials, enforce MFA everywhere, and remove unused third-party apps.

Legacy & EOL Gear Lifecycle

Retire legacy servers and segment building systems and management interfaces.

Evolving Social Engineering Awareness

Train all staff on calendar, device-code, ClickFix, and help desk lures; verify banking changes.

Zero-Day Emergency Patching

Patch KEV-listed flaws within days and check for compromise after zero-day patches.

Third-Party & Open-Source Audits

Question vendors and MSPs on data transfer and app permissions; add patch and notice terms.

Log Monitoring & Incident Readiness

Alert on device-code sign-ins and new app secrets; validate immutable backups.

K-12 Breach Sources (district incidents)

Spokane Public Schools (Spokane, WA) · Jerome Joint SD No. 261 (Jerome, ID) · Easthampton Public Schools (Easthampton, MA) · Indiana Area SD (Indiana, PA) · North Slope Borough SD (Utqiaġvik, AK) · Lakin USD 215 (Lakin, KS) · Adams-Friendship Area SD (Adams, WI) · Alisal Union SD (Salinas, CA) · Tulare Joint Union HSD (Tulare, CA) · ICEF Public Schools (Los Angeles, CA) · Slate Valley UUSD (update, VT). Plus 8 unconfirmed leak-site claims.

Full details, indicators, and references are in the complete October 2026 report. To apply this data to your district's needs, contact the LTC vCISO Program.