Learning Technology Center

vCISO Program

Monthly Cyber Threat Intelligence

October 2026

Compiled by Technology Learning Center, vCISO Program

Covers September 20, 2026 to October 19, 2026

Table of Contents

Table of Contents 2
Introduction 4
Threat Landscape for October 2026 4
Monthly Areas of Focus 5
- Citrix NetScaler — Three Zero-Days Exploited, Education Among Victims (CVE-2026-88771 / 88772 / 88779) 5
- Frontline Education Breach — School Employee and Applicant Data Exposed 5
- California State Testing Breach — One Stolen Credential, Millions of Student Records 6
- Microsoft — Record Patch Tuesday, Exploited Windows Shell and SharePoint Flaws, Exchange Fix 7
- Remote-Access and Network Infrastructure — Cisco, SonicWall, and Ivanti 7
- ConnectWise Cloud Backup Suspended — Attackers Abused Trusted Microsoft 365 Apps 8
- Phishing Beyond the Inbox — Device Codes, Calendar Invites, and Help Desk Calls 9
- Endpoint Defense Evasion — Fake Installers, ChatGPT-Hosted ClickFix, and Defender Tampering 9
- Apple CoreGraphics Zero-Day — iPads and Macs (CVE-2026-86950) 10
- Website Platforms — WordPress Core Flaw Exploited Within Hours, Critical Drupal Fixes 10
- AI-Driven Attacks Move From Research to Real Intrusions 11
- Building and Physical Systems Become Ransomware Targets 11
- Old and Overlooked Software — LibreOffice, Legacy KEV Additions, and Adobe 12
- Law Enforcement Pressure — ShinyHunters Arrests, KillSec Takedown, and a Fraudulent "Recovery" Firm 12
- Platform Changes and Planning Items 13

K-12 District Incidents 13
- Confirmed or Press-Reported Incidents 14
  - Spokane Public Schools, Spokane, WA 14
  - Jerome Joint School District No. 261, Jerome, ID 14
  - Easthampton Public Schools, Easthampton, MA 14
  - Indiana Area School District, Indiana, PA 14
  - North Slope Borough School District, Utqiaġvik, AK 14
  - Lakin USD 215, Lakin, KS 14
  - Adams-Friendship Area School District, Adams, WI 15
  - Alisal Union School District, Salinas, CA 15
  - Tulare Joint Union High School District, Tulare, CA 15
  - Inner City Education Foundation (ICEF Public Schools), Los Angeles, CA 15

Update: Slate Valley Unified Union School District, VT 15
Ransomware Leak-Site Claims (Not Publicly Confirmed) 15
Vendor and State-Level Incidents Affecting Multiple Districts 16
Patterns 16
Conclusion 16
Recommendations 17
Immediate Perimeter & Credential Remediation 17
Credential Audit 17
Zero-Day Emergency Patching 17
Infrastructure & Asset Governance 17
Legacy & EOL Gear Lifecycle 17
Third-Party & Open-Source Audits 18
Detection & Human Element Safeguards 18
Evolving Social Engineering Awareness 18
Log Monitoring & Incident Readiness 18
LTC vCISO Program 19
References 20
K-12 District Incidents 20
Vendor Breaches (Frontline, ETS) 21
Vulnerabilities and Patching 22
Identity, Cloud, and Third-Party Access 23
Malware, Evasion, and AI 24
Law Enforcement and Industry 24
Executive Summary 26

Introduction

The mission of the Learning Technology Center (LTC) in Illinois is to empower K-12 public school districts, schools, and educators through technology services, strategic consulting, and professional learning to improve educational opportunities for all students. In pursuit of that mission, the vCISO Program compiles this monthly intelligence analysis to provide K-12 technology leaders with actionable risk insights.

The October 2026 reporting period is defined by risk that arrives through someone else's door. The two largest K-12 data exposures of the month came from vendors, not district networks: a stolen login at California's state testing contractor exposed records on millions of students, and a flaw in software used by Frontline Education exposed employee Social Security numbers across several states. At the same time, at least 18 US K-12 schools and districts were hit by cyberattacks or listed as targets, and attackers continued to break remote-access appliances before patches existed.

Threat Landscape for October 2026

September proved the back-to-school window was dangerous. October showed the risk has not eased now that school is in session. Between September 20 and October 19, we tracked 10 confirmed or press-reported incidents at US K-12 schools and districts, 8 more schools listed only on ransomware leak sites, and 4 vendor or state-level incidents that touched many districts at once. Jerome, Idaho closed schools for two days after attackers reached cameras, door locks, and HVAC. Spokane, Washington lost its student information and payroll systems for roughly two weeks and now believes student and staff data were taken. Easthampton, Massachusetts ran on paper.

The dominant theme is third-party and identity risk. The California Department of Education disclosed that a single compromised credential on a testing vendor's file-transfer site let an attacker copy statewide assessment files for almost four months, including disability, Section 504, and English-learner data. Frontline Education, whose HR and workforce software is used across K-12, notified districts that employee and applicant data had been exposed via an unnamed third-party product. ConnectWise suspended its Microsoft 365 backup service after attackers abused its own application identities to sign in to customer tenants. This aligns with the trend in Clever's Cybersecure 2026 survey (published in March), in which third-party breaches rose from 4% of district-reported breaches in 2023 to 32% in 2025.

The edge of the network remains under steady fire. Citrix NetScaler suffered three zero-days in two weeks, with education named among victim sectors. Flaws in Cisco SD-WAN, SonicWall SMA 1000, Ivanti Connect Secure, and Microsoft SharePoint were all exploited or targeted within days of disclosure. Microsoft's October Patch Tuesday fixed a record 1,413 CVEs, including a Windows Shell zero-day that bypasses the protection Windows applies to downloaded files.

Two broader forces sit behind all of this. First, AI is now part of real intrusions, not just research: an AI agent ran a live breach of a Dutch security nonprofit, a threat actor used AI agents to delete more than 100 Azure storage accounts in about seven minutes, and the UK's National Cyber Security Centre warned that AI is set to help attackers more than defenders. Second, law enforcement is applying real pressure: arrests tied to ShinyHunters (the group behind the Canvas breach) and the takedown of the KillSec ransomware operation. Arrests do not return stolen data, and members of disrupted groups often rebrand. For Illinois districts, the takeaway is to hold vendors accountable, tighten identity controls on people and applications, and patch internet-facing systems on a days-not-weeks timeline.

Monthly Areas of Focus

Citrix NetScaler – Three Zero-Days Exploited, Education Among Victims (CVE-2026-88771 / 88772 / 88779)

Severity: Critical

What happened: Citrix disclosed two remote code execution flaws in NetScaler ADC and Gateway that were exploited before any patch existed: CVE-2026-88771 (CVSS v4 9.5, unauthenticated command execution in the default configuration) and CVE-2026-88772 (CVSS v4 9.5, memory overflow when DTLS is enabled, which is the default for VPN virtual servers). Rapid7 saw the first exploitation attempts on September 20, and CISA added both to its Known Exploited Vulnerabilities (KEV) catalog on September 27. A third flaw, CVE-2026-88779 (CVSS v4 8.7) in SAML processing, was added to KEV on October 4. Mandiant identified likely victims in North America and Europe, including the education sector, and attackers are attempting to install web shells. The US and Australia issued joint warnings. The first round of fixes (14.1–73.37) did not cover CVE-2026-88779.

K-12 relevance: NetScaler Gateway is a common remote-access front end for districts and regional offices of education. It is exactly the kind of edge device ransomware operators target first, and education is a confirmed victim sector in this campaign.

Recommended action: Upgrade to 14.1–73.41 or 13.1–64.28 (or the matching FIPS/NDcPP builds), which fix all three exploited flaws. Because these were exploited before patches existed, patching alone does not prove the appliance is clean: preserve evidence, run Citrix's indicator-of-compromise script before upgrading, hunt for web shells, and rotate session tokens, certificates, and credentials if anything looks suspicious. Keep the management interface off the internet. Branch 13.1 reached end of maintenance September 15; plan the move to 14.1.

Frontline Education Breach – School Employee and Applicant Data Exposed

Severity: Critical

What happened: Frontline Education, which provides HR, absence management, applicant tracking, and health services software to K-12 districts, began notifying districts around October 1 that attackers had exploited a vulnerability in "a third-party software product" it uses. Frontline says the flaw was identified August 14. Exposed data includes employee Social Security numbers, email and home addresses, and in some filings driver's license numbers; applicant tracking data was also affected. In South Carolina, districts were told student health services data (medical and billing records) may have been involved, while Frontline says no Texas student data was exposed. Named districts include Klein, Lubbock, Waco, Fort Worth, Crowley, and Laredo ISDs in Texas (Klein's filing alone lists about 37,966 people), Anderson School Districts 2, 3, and 5 and Greenwood 50 in South Carolina, and Farmington Public Schools in Connecticut (2,129 employees). Frontline has not named the third-party product or released a total count. It is offering two years of credit monitoring, and individual letters are expected to begin around October 26. No Illinois districts had been publicly named as of this writing.

K-12 relevance: This is a K-12 vendor breach touching HR, hiring, and student health data. Frontline is widely used in Illinois, so many districts may be affected, and exposed staff SSNs and addresses are ideal fuel for payroll diversion, W-2, and tax fraud schemes.

Recommended action: Confirm which Frontline modules your district uses and whether you received a notice (legitimate notices came from frontline@notifications.cyberscout.com). Ask Frontline in writing for your affected record counts, the data types involved, and the name of the third-party product. Review Illinois PIPA obligations and SOPPA, if any student data was involved, against your data privacy agreement. Warn staff about follow-on phishing attempts and require call-back verification to a number on file before any direct deposit or banking change.

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

Severity: High

What happened: On October 16, the California Department of Education (CDE) announced that an unauthorized party used a compromised login on a file-transfer (SFTP) site run by Educational Testing Service (ETS), the state's contractor for the CAASPP and ELPAC assessments. Files were copied from May 22 to September 18, 2026, nearly four months without detection. ETS discovered the activity September 25, and districts were notified October 2. No exact count has been released; reporting describes "millions" of current and former students, with some records reaching back to 2006. Exposed data includes name, statewide student ID, date of birth, address, school, grade, demographics, primary language, English-learner status, disability and Section 504 status, federal program eligibility, and assessment results. Social Security numbers, financial data, and parent information were not exposed. ETS rebuilt the site and is offering two years of identity monitoring.

K-12 relevance: Illinois districts and ISBE also exchange assessment and student data with contractors through file-transfer systems. A single credential without strong protection exposed the most sensitive categories of student data, including special education status, at statewide scale. Districts cannot patch their way out of a vendor's weak login.

Recommended action: Inventory all of your data exchange pathways. Ask your assessment, SIS, and data-integration vendors how student data is transferred and stored: is multi-factor or key-based authentication required on SFTP accounts, are accounts restricted by IP address, are transfers logged and reviewed, and how long are files retained? Remove stale files from district-side SFTP drop folders. Check data privacy agreements for breach-notification timelines, and prepare family messaging for the phishing that typically follows a large breach announcement.

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

Severity: Critical

What happened: Microsoft's October 13 Patch Tuesday fixed a record 1,413 CVEs. It included CVE-2026-96951 (CVSS 8.8), an exploited Windows Shell security feature bypass that defeats Mark of the Web, the label Windows uses to warn about and restrict files downloaded from the internet or received as attachments. CISA added it to KEV on October 13, alongside Ivanti Connect Secure CVE-2026-104935. Separately, the SharePoint Server flaw CVE-2026-65660, initially described as a moderate spoofing issue, turned out to be an authenticated remote code execution and was exploited in late September (KEV, September 25); it was fixed in the August updates and can be chained with a June authentication bypass that allows anonymous access. Symantec also reported the China-linked Warlock ransomware operators using older SharePoint "ToolShell" flaws against a university and critical infrastructure. Microsoft issued an out-of-band fix for on-premises Exchange (CVE-2026-96940, CVSS 8.8) that let any user in an organization read other users' mailboxes. Windows Server 2022 reached the end of mainstream support on October 13; security updates continue through October 2031.

K-12 relevance: Phishing attachments are the most common way attackers get into district endpoints, and this zero-day removes a built-in defense against them. Many districts still run on-premises SharePoint or hybrid Exchange for intranets, document storage, and email, where any compromised staff or student account could read superintendent, HR, or special education mail.

Recommended action: Deploy October cumulative updates to all Windows endpoints and servers now (for example, Windows 11 24H2 build 26100.9711 or later). Apply the June and August SharePoint updates, disable anonymous access, hunt for web shells in the LAYOUTS directory, and rotate ASP.NET machine keys if compromise is suspected; retire SharePoint 2013. Install the "September 2026 v2" Exchange security update on every Exchange server and every machine with Exchange Management Tools. Enable Attack Surface Reduction rules that block scripts and executables launched from user-writable folders. Add Windows Server 2025 migration to the FY27-28 budget.

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

Severity: High

What happened: Cisco disclosed CVE-2026-76504 (CVSS 9.8), an exploited authentication bypass in Catalyst SD-WAN Manager that gives an unauthenticated attacker admin-level API access; CISA added it to KEV September 30, and it is the fifth exploited SD-WAN zero-day of 2026. Cisco also patched critical flaws in Nexus 3000/9000 switches, including CVE-2026-76471 (CVSS 9.8; root code execution via the NX-API, which is off by default), and four critical flaws in Cisco License (formerly Smart Software Manager). SonicWall fixed CVE-2026-102255 (CVSS 10.0), a pre-authentication server-side request forgery flaw in SMA 1000 appliances; exploitation attempts began October 8, two days after the patch, though success has not been confirmed. Ivanti Connect Secure CVE-2026-104935 (CVSS 8.6) was added to KEV October 13. KillSec, the ransomware group dismantled this month, relied heavily on poorly secured edge devices.

K-12 relevance: Districts and consortia depend on these products for remote access and core switching. Small IT teams often cannot patch appliances within days, and attackers now begin exploiting within hours to days of disclosure.

Recommended action: Upgrade Catalyst SD-WAN Manager to the first fixed release for your train (for example 20.12.8.2, 20.15.6.1, or 20.18.4.1) and review service-proxy logs for j_security_check requests from unknown addresses. Update SonicWall SMA 1000 to 12.4.3-03670 or 12.5.0-03082 and rotate credentials and TOTP seeds if compromise is suspected. Patch Ivanti Connect Secure to 25.1.3.0. On Nexus switches, disable NX-API, NGOAM, and MPLS OAM where unused and apply fixed releases. Put all management interfaces on a restricted VLAN reachable only through VPN with MFA.

ConnectWise Cloud Backup Suspended - Attackers Abused Trusted Microsoft 365 Apps

Severity: High

What happened: ConnectWise detected on October 14 that attackers had gained access to its application identities and used them to sign in to customers' Microsoft 365 tenants. Affected services include Cloud Backup (formerly SkyKick) and several Cloud Management apps. Huntress observed sign-ins from the malicious infrastructure to almost 1,000 tenants, about 300 of them successful, and confirmed follow-on activity in at least two, including a Global Administrator grant and new application secrets. ConnectWise disabled seven application identities, suspended Cloud Backup on October 17, and completed a credential reset October 20; restoration has no date. Disabling the apps does not undo changes already made in a tenant. In a related pattern, Meta disclosed that a stolen employee credential gave attackers access to its GitHub repositories, and Microsoft described a threat actor (Storm-3168, also called JadePuffer) using a service principal secret leaked in a public GitHub issue to destroy Azure resources.

K-12 relevance: Many districts rely on managed service providers who install third-party backup and management apps with broad permissions into the district's Microsoft 365 tenant, sometimes long after the service stopped being used. Those apps can read FERPA-covered mail and files, and many districts do not know they are there. Districts using this service currently have no scheduled Microsoft 365 backups.

Recommended action: Ask your MSP directly whether ConnectWise or SkyKick apps exist in your tenant, including dormant ones. Preserve and review Entra ID sign-in and audit logs since October 13, including sign-ins from 144.172.64.128, 144.172.64.99, and 144.172.64.60. Audit enterprise applications and service principals for new secrets or certificates, admin role grants, consent grants, mailbox forwarding, and inbox rules. Remove unused third-party apps, limit who holds Application Administrator roles, and arrange temporary alternate backup coverage. Scan district GitHub organizations for exposed secrets and require SSO and MFA.

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

Severity: High

What happened: The Wazza phishing kit, documented by ANY.RUN and LevelBlue, abuses Microsoft's device-code sign-in flow: victims enter a code on a real Microsoft page, which hands the attacker a session without stealing a password. Lures use Adobe, DocuSign, and OneDrive themes, and are often sent from already-compromised partner accounts. Security firms also report calendar-invite phishing growing rapidly: malicious invites land directly on calendars even when the email goes to spam, with "new voicemail," invoice, and fake internal meeting lures linking to fake Google, Microsoft, or PayPal login pages or fake support numbers. Astrana Health disclosed a breach that began when attackers spoofed the company's main phone number and called employees to obtain access. In South Carolina, phishing emails impersonating the state education department and its ClassWallet payment platform diverted about $100,000 from the Education Scholarship Trust Fund. The Pentagon's personnel system breach (about 3 million people) will add fuel for targeted phishing against veteran and military-family staff.

K–12 relevance: Staff calendars in Google Workspace for Education and Microsoft 365 are trusted spaces, and voicemail and meeting lures fit school routines. Business office and payroll staff remain prime targets for payment and banking-change fraud, as the Adams-Friendship (WI) loss this month shows.

Recommended action: Block the device-code authentication flow with Entra Conditional Access, allowing exceptions only for devices that need it, such as meeting-room systems, and alert on device-code sign-ins. In Google Workspace, set external calendar invitations to appear only from known senders or after acceptance; review automatic calendar processing in Exchange. Tell staff to delete or report suspicious invites rather than decline them. Give the help desk a caller-verification script with call-back to a number on file, and require dual approval for any vendor payment or banking change.

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

Severity: High

What happened: Attackers used search-optimized fake GitHub repositories impersonating LastPass and at least 39 other vendors to deliver a signed kernel driver that kills 145 security

products, including EDR agents, followed by the Rapuncel information stealer, which takes passwords from 25 browsers. Huntress documented sponsored Google results for "chatgpt" leading to malicious Custom GPTs on chatgpt.com that pushed a fake CAPTCHA "ClickFix" lure, tricking users into pasting a PowerShell command that installed a remote access trojan; at least 40 people were infected. Securonix described TASK#STOMP, a PowerShell backdoor that hides in scheduled tasks with names such as "Network Audio Service" and steals documents, Wi-Fi passwords, and clipboard data. A researcher also released BigDiskBuster, a proof of concept that stops Microsoft Defender from receiving signature updates; Microsoft says Defender now detects it. Cisco Talos described CLOSEDQUORUM, a Windows implant that asks several commercial AI models to vote on its next action, although in-the-wild use is not confirmed.

K-12 relevance: Teachers and students search for ChatGPT and popular tools every day, and ClickFix remains one of the leading ways school endpoints are infected. Many districts rely on Microsoft Defender as their only endpoint protection, so tools that silently blind it or stop its updates weaken every other control.

Recommended action: Remove local admin rights and require software installation from a managed catalog (Intune Company Portal or equivalent). Turn on Microsoft's vulnerable driver blocklist, memory integrity (HVCI), and Defender tamper protection. Restrict PowerShell and the Run dialog for standard users and students. Monitor fleet-wide Defender signature age and alert when definitions are more than three days old. Teach staff that no legitimate website will ask them to paste a command to "verify" they are human, and bookmark approved AI tools.

Apple CoreGraphics Zero-Day – iPads and Macs (CVE-2026-86950)

Severity: High

What happened: Apple patched CVE-2026-86950, an out-of-bounds write in CoreGraphics that can run attacker code when a crafted file is opened. Apple said it may have been exploited in an "extremely sophisticated attack" against specific individuals. CISA added it to KEV on September 29. A day later, researchers released a public proof of concept using a malicious PDF font, which raises the risk of broader use. Fixes are in iOS and iPadOS 26.7.1, macOS Tahoe 26.7.1, and macOS Sequoia 15.8.1.

K-12 relevance: Districts manage large iPad and Mac fleets for students and staff, and PDFs are everywhere in schools. Superintendents and other leaders are the kinds of targeted individuals these exploits are first used against.

Recommended action: Use your MDM (Jamf, Mosyle, Intune, or similar) to require iOS/iPadOS 26.7.1 and macOS 26.7.1 or 15.8.1 as minimum versions, report on devices below the minimum, and isolate or retire devices that cannot update.

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

Severity: High

What happened: WordPress core flaw CVE-2026-87902 (CVSS 9.2), an unauthenticated path traversal that can lead to code execution under certain server configurations, affects versions 4.7.0 through 7.1.1. Patchstack saw attacks less than five hours after the September 22 fix in 7.1.2 (backported to older branches), and activity grew tenfold as public scanners circulated. Drupal released fixes on October 14 for CVE-2026-108097, a critical Field UI flaw, and warned that exploits could emerge within hours or days; fixed versions are 10.6.19, 11.3.19, and 11.4.10.

K-12 relevance: This is the third straight month of critical WordPress risk after August's core flaw and September's Avada theme flaw. District, school, PTO, booster, and alumni sites often run on shared hosting with no clear owner for updates, and a compromised public website can be used to deface the district or phish families.

Recommended action: Update WordPress to 7.1.2 (or the patched release for your branch) and enable automatic core updates. Check web server logs for traversal requests and look for unexpected PHP files in /tmp. Update Drupal to a fixed release, or uninstall the Field UI module if you cannot update immediately. As we said in August, every district-associated site needs a named owner; sites without one should be retired or moved to a managed platform.

AI-Driven Attacks Move From Research to Real Intrusions

Severity: Medium

What happened: The Dutch Institute for Vulnerability Disclosure (DIVD), a cybersecurity nonprofit, was breached through two zero-days in the open-source Zammad help desk (CVE-2026-102489 and CVE-2026-102490), after which an AI agent chose and narrated its own next steps inside the network; segmentation limited the damage. Microsoft and Sysdig described Storm-3168 (JadePuffer) using AI agents to map an Azure environment and delete most of more than 100 storage accounts in about seven minutes; resources protected by Azure delete locks survived. Lumen's Black Lotus Labs found the PoeLLM botnet compromising roughly 2,200 to 3,400 exposed self-hosted AI servers (Lumen's report cites both figures) (Ollama, LiteLLM, and similar tools) for cryptomining and proxying. The UK National Cyber Security Centre warned that AI is set to help attackers more than defenders, and a PwC survey found only 17% of organizations assign AI security to the CISO.

K-12 relevance: In July we reported on JadePuffer and the shrinking time from intrusion to impact; this month that trend is visible in real breaches. Districts and staff are also experimenting with self-hosted AI tools in computer science and CTE labs, often exposed to the internet with default settings.

Recommended action: Inventory any self-hosted AI tools (Ollama, LiteLLM, Open WebUI and similar) and remove them from the public internet. Find and upgrade any Zammad instance to version 7. Apply Azure delete locks and soft delete to storage and Key Vaults, and move service principals from long-lived secrets to managed identities. Name an owner for AI risk in the district, and keep humans approving automated changes to production systems.

Building and Physical Systems Become Ransomware Targets

Severity: Medium

What happened: In Jerome, Idaho, attackers reached district surveillance cameras, electronic door locks, and HVAC controls, closing schools for two days and demanding a ransom. In France, attacks targeting internet-exposed refrigeration and building controllers (Danfoss, Copeland, and Dixell) disrupted roughly 700 supermarkets in a single night, and the national CERT issued a broader warning on October 13. North Slope Borough, Alaska lost school phone service across the district. Richmond Public Schools in Virginia also reported a network shutdown affecting cameras and phones on October 21, just after this reporting period.

K-12 relevance: District HVAC, kitchen refrigeration, door access, and camera systems are often managed by contractors and reachable from the internet or the general network. When they fail, the incident becomes a student- and food-safety event, not only a data event.

Recommended action: Inventory building automation, access control, camera, and refrigeration controllers. Remove internet-facing management interfaces and require contractor access through VPN or a jump host with named accounts and MFA. Segment these systems from general IT. Make sure doors can be secured and temperature alarms monitored independently of the network, and test how buildings operate when phones and cameras are down.

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

Severity: Medium

What happened: A malicious spreadsheet can run attacker code in LibreOffice (CVE-2026-63277) and Apache OpenOffice (CVE-2026-59265) without a macro warning when Java support is enabled; a public proof of concept exists. Fixes are LibreOffice 26.2.5 or 26.8.0 and OpenOffice 4.1.17. CISA added five old flaws to KEV in connection with a seven-nation advisory on China-linked activity: ProFTPD (CVE-2015-3306), ONLYOFFICE Docs (CVE-2021-3199), Strapi (CVE-2023-22894), Apache Struts (CVE-2016-3081), and ISC BIND (CVE-2015-5477). Adobe fixed roughly 140 vulnerabilities across 10 products, including critical ColdFusion flaws; none were reported as exploited.

K-12 relevance: Free office suites are common on lab images, Linux machines, and staff home computers, and old FTP, DNS, and Java web servers tend to survive in district environments long after their owners leave. Photoshop and Bridge run in art and media labs.

Recommended action: Update LibreOffice and OpenOffice, and disable Java in those suites where it is not needed. Scan for ProFTPD, ONLYOFFICE Docs, Strapi, Apache Struts, and BIND, then upgrade or retire them. Push Creative Cloud updates, and patch ColdFusion first if any legacy district application still uses it.

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

Severity: Medium

What happened: US authorities arrested a suspect tied to ShinyHunters following the group's breach of the FBI's job applicant portal, which ran on Oracle PeopleSoft; Reuters reported that an Accenture contractor was removed after failing to apply a security patch. Other suspected members were arrested in the Netherlands and detained in Jordan. ShinyHunters is the group behind this year's Canvas/Instructure breach and claimed September's Mathspace breach, and Google reported its PeopleSoft campaign hit more than 100 organizations, 68% of them in higher education. In Operation KillSwitch, police in ten countries dismantled the KillSec ransomware group, arresting three people and seizing its leak site and servers. The Justice Department charged the owner of MonsterCloud, a ransomware "recovery" firm accused of secretly paying more than $8 million in ransoms while billing clients more than $19 million for supposed decryption.

K-12 relevance: The groups that have hit education hardest this year are under pressure, but arrests do not return stolen data, and members often reappear under new names. The FBI breach and MonsterCloud case are both vendor-trust lessons: a missed patch by a contractor, and a recovery firm that quietly paid criminals.

Recommended action: Re-check exposure on Canvas, PowerSchool, and other SaaS platforms. If the district or a partner runs PeopleSoft, confirm Oracle's patch for CVE-2026-35273 is applied, not only the workaround. Pre-select a vetted incident response firm through your cyber insurer or a state partner, and require written disclosure of any payment made to an attacker.

Platform Changes and Planning Items

Severity: Low

What happened: Microsoft Teams will let admins customize the list of blocked file types starting in November (the base "weaponizable file protection" feature is available now but off by default). Outlook on the web and the new Outlook will block .msix and .msixbundle attachments by mid-November. Attackers hijacked three country-code domain registries to obtain fraudulent HTTPS certificates for Google domains, a reminder that DNS compromise defeats the browser padlock. Cloudflare announced it will become a public certificate authority, including post-quantum certificates in 2027. Google partially reversed its Chrome bug bounty cuts.

K-12 relevance: These are low-cost hardening wins and planning signals for Microsoft 365 districts and any district managing its own domain.

Recommended action: Enable Teams file-type checking now (Teams admin center > Messaging settings > Messaging safety). Leave the Outlook MSIX block in place and add it at your mail gateway. Turn on registrar lock and MFA for the district domain registrar, publish CAA records, and monitor Certificate Transparency logs for unexpected certificates. Keep a list of certificates and their expiration dates, and start a simple cryptography inventory for post-quantum planning.

K-12 District Incidents

Between September 20 and October 19, 2026, we identified 18 US K-12 schools and districts with new cyber incidents or ransomware claims: 10 confirmed by the school or reported by the press, and 8 that so far appear only on ransomware leak sites. Slate Valley, Vermont, reported last month, also appeared on a new leak site. Four further vendor or state-level incidents affected many districts at once. Leak-site claims are made by criminals, are sometimes exaggerated or wrong, and are listed here for awareness only.

Confirmed or Press-Reported Incidents

Spokane Public Schools, Spokane, WA

The district detected a network security incident on September 20 and took online systems offline, including PowerSchool and its BusinessPlus payroll system. Schools stayed open. Both systems were restored by early October, and on October 8 the district said it had reason to believe student and staff data were compromised. No threat actor, ransom demand, or count of affected people has been disclosed; notification letters are pending.

Jerome Joint School District No. 261, Jerome, ID

Detected Saturday, October 17. The attack reached the district network, surveillance cameras, electronic door locks, and HVAC, and took district communications offline. Schools closed October 19 and 20 and reopened October 21. Attackers demanded a ransom and threatened to leak data. Reports conflict on whether student data was accessed; the superintendent said student data and devices are secure.

Easthampton Public Schools, Easthampton, MA

Suspicious activity was spotted on October 5. The district shut down all online systems, taking out phones, email, Wi-Fi, and classroom technology, and kept schools open using paper attendance. ParentSquare remained available for family communication, and Springfield Public Schools, itself recovering from a September attack, lent wireless modems. A forensic review through the district's cyber insurer is under way.

Indiana Area School District, Indiana, PA

Announced October 4. A local server and classroom desktops were affected, and lunch payments were disrupted; students were asked to bring Chromebooks. The district says PowerSchool and its intermediate unit's systems show no sign of compromise. The insurer engaged forensics and legal teams, and the district was not fully restored as of October 16.

North Slope Borough School District, Utqiaġvik, AK

An outage beginning September 8 left schools across the district without phone service. The district's domain appeared on the INC Ransom leak site September 27, and an October 5 letter warned employees that personal information, potentially including Social Security numbers and benefits data, may have been accessed. The district is working with the FBI and offering identity monitoring to students and staff.

Lakin USD 215, Lakin, KS

Announced October 14. The district shut down Wi-Fi to contain a breach it says was limited to a copier server and reports that no student or staff data was accessed. Systems were restored the same day. (Limited public detail available.)

Adams-Friendship Area School District, Adams, WI

The business manager was placed on leave October 16, and the loss became public October 22, just after this reporting period. About $92,000 was lost when a payment request the bank had flagged as unusual was processed anyway. The district has contacted law enforcement and its insurer. Wisconsin's Department of Public Instruction counts more than 40 cyberattacks on Wisconsin schools so far in 2026.

Alisal Union School District, Salinas, CA

Filed breach notification letters with the California Attorney General on October 7 for unauthorized access discovered in June. The number of people affected has not been disclosed.

Tulare Joint Union High School District, Tulare, CA

The Booba Project group listed Tulare Western High School on its leak site on September 22, claiming to have 35 GB of administrative data, and the district filed a breach notification with the California Attorney General on October 13. The connection between the two has not been confirmed by the district.

Inner City Education Foundation (ICEF Public Schools), Los Angeles, CA

This charter network filed a California Attorney General breach notice around October 16 for incidents dated in 2024, which is a late notification. Details have not been disclosed.

Update: Slate Valley Unified Union School District, VT

Reported last month. The board voted on September 28 not to pay the ransom, and the Kairos group then listed the district on October 1, claiming to have 647 GB of data, including student and employee personal and medical data.

Ransomware Leak-Site Claims

School / District	Location	Group	Listed	Notes
Llano ISD	Llano, TX	Qilin	Oct 18	No district statement verified
Seminole Public Schools	Seminole, OK	Global Secret Group	Oct 19	Group claims 39.6 GB
Ansonia Public Schools	Ansonia, CT	The Gentlemen	Oct 9	No data size given
Santee School District (Foundation)	Santee, CA	The Gentlemen	Oct 9	Listed under district domain
The New Community School (private)	Richmond, VA	INC Ransom	Oct 7	Serves students with dyslexia
Friendship Christian School (private)	Unconfirmed	Qilin	Oct 11	Exact school not identified

Slate Valley Unified Union SD (update)	Fair Haven, VT	Kairos	Oct 1	Claims 647 GB; board refused ransom

Vendor and State-Level Incidents Affecting Multiple Districts

- **ETS / California state testing:** One compromised credential on a vendor SFTP site exposed assessment, demographic, and disability data on millions of current and former California students (see Areas of Focus).
- **Frontline Education:** Employee, applicant, and some student health data exposed through a third-party software flaw; districts named in Texas, South Carolina, and Connecticut. Kern County Superintendent of Schools (CA) filed a notice with the same August 14 breach date (see Areas of Focus).
- **South Carolina Department of Education:** Phishing impersonating the department and ClassWallet stole provider logins and diverted about $100,000 from the Education Scholarship Trust Fund, delaying tuition payments to private schools.
- **Maryland State Department of Education:** Took its website offline on October 7 during a cybersecurity investigation; no data impact disclosed.

Patterns

- **Vendors caused the widest damage.** The two largest exposures (ETS and Frontline) reached millions of students and tens of thousands of employees without any district network being breached.
- **Small, rural, and private schools are being listed quietly.** Eight of the 18 schools appear only on leak sites, with no public acknowledgment. Qilin led claims this month, followed by The Gentlemen and INC Ransom.
- **Physical systems are now in scope.** Cameras, door locks, HVAC, and phones failed in Jerome, North Slope, and Richmond, turning data incidents into safety and closure events.
- **Recovery takes weeks, and payment fraud continues.** Most districts stayed open on paper while recovery stretched for weeks, and two incidents (Adams-Friendship and South Carolina) were payment diversion, not ransomware.

Conclusion

October showed that a district's risk now extends well beyond its own network. The month's largest student and staff data exposures came from a testing contractor and an HR software vendor, Microsoft 365 tenants were entered through a trusted backup provider's own apps, and the remote-access appliances districts depend on were exploited before patches existed. Meanwhile, ransomware groups continued to list schools across the country, and attacks on

cameras, locks, and HVAC made clear that a cyber incident can become a building safety event. The path forward is the same set of fundamentals, applied to vendors and applications as rigorously as to staff: strong identity controls, fast patching of exploited flaws, segmentation, and contracts that give districts real visibility when a partner fails.

Recommendations

Immediate Perimeter & Credential Remediation

Credential Audit

- Rotate administrative and remote-access credentials, session tokens, and certificates for Citrix NetScaler, SonicWall SMA 1000, Cisco SD-WAN Manager, and Ivanti Connect Secure if they were exposed before patching.
- Enforce MFA on all remote management access points, SFTP and data-transfer accounts, domain registrar accounts, and GitHub organizations.
- Block the device-code authentication flow in Entra ID except where required, alert on device-code sign-ins and new MFA registrations, and require phishing-resistant MFA for IT, business office, HR, and leadership accounts.
- Audit Microsoft 365 and Google Workspace third-party applications and service principals: remove unused apps (including dormant ConnectWise/SkyKick apps), review new secrets and admin role grants, and limit Application Administrator roles.

Zero-Day Emergency Patching

- Apply priority patches for Citrix NetScaler (14.1–73.41 / 13.1–64.28), Microsoft October cumulative updates (CVE-2026–96951), SharePoint (CVE-2026–65660), Exchange (CVE-2026–96940), Cisco Catalyst SD-WAN (CVE-2026–76504), SonicWall SMA 1000 (CVE-2026–102255), Ivanti Connect Secure (25.1.3.0), Apple iOS/iPadOS/macOS 26.7.1, WordPress 7.1.2, and Drupal 10.6.19 / 11.3.19 / 11.4.10.
- Track CISA KEV additions and prioritize by actual exploitation and EPSS, not CVSS alone; set a documented patch window measured in days for internet-facing systems and KEV-listed flaws.
- After patching anything that was exploited as a zero-day, check for compromise: run vendor IoC scripts, hunt for web shells, and review logs from before the patch.

Infrastructure & Asset Governance

Legacy & EOL Gear Lifecycle

- Identify and isolate end-of-life systems: SharePoint 2013, Exchange 2016/2019, NetScaler 13.1, and legacy ProFTPD, BIND, Struts, ONLYOFFICE, ColdFusion, and Zammad servers. Upgrade or retire them.

- Restrict management interfaces for firewalls, VPN appliances, switches, building automation, cameras, and door access from direct exposure on the public internet, and place them on a management VLAN reachable only by VPN with MFA.
- Segment building automation, HVAC, refrigeration, door access, cameras, and VoIP from general IT, and require named, MFA-protected contractor access.
- Begin Windows Server 2025 migration planning for FY27–28 and start a certificate and cryptography inventory for post-quantum readiness.

Third-Party & Open-Source Audits

- Ask Frontline, assessment vendors, SIS providers, and data-integration partners how student and staff data is transferred and protected (MFA or key-based SFTP, IP restrictions, logging, retention), and request affected-record details for any notice received.
- Add contract and data privacy agreement language requiring critical-patch timelines, post-patch compromise assessments, defined breach notification windows, log access, and disclosure of any payment made to an attacker.
- Ask your MSP which third-party apps they have installed in your tenant and what permissions they hold; arrange alternate Microsoft 365 backup if you use ConnectWise Cloud Backup.
- Establish monitoring and rapid patch protocols for open-source systems in use, including WordPress, Drupal, LibreOffice, Zammad, and self-hosted AI tools such as Ollama and LiteLLM; remove AI servers from the internet.

Detection & Human Element Safeguards

Evolving Social Engineering Awareness

- Expand awareness training beyond email phishing to cover calendar-invite phishing, device-code prompts, "paste this command" ClickFix pages (including ones hosted on chatgpt.com), fake software downloads, and help desk impersonation calls with spoofed caller ID.
- Warn staff about follow-on phishing and payroll fraud after the Frontline and Pentagon breaches; require call-back verification and dual approval for any banking or direct-deposit change.
- Give the help desk a caller-verification script, and tell staff to delete or report suspicious calendar invites rather than decline them.
- Include teachers, not just office staff, in security awareness; classroom staff are frequent targets and are often missed by training programs.

Log Monitoring & Incident Readiness

- Enhance central logging and alerting to detect device-code sign-ins, new service principal secrets and admin role grants, bursts of Azure delete operations, Defender signature age over three days, new kernel driver services, and PowerShell launched from Office or Explorer.

- Turn on Microsoft's vulnerable driver blocklist, memory integrity, Defender tamper protection, and Attack Surface Reduction rules; remove local admin rights.
- Validate offline, immutable backups, including the SIS, payroll, and Microsoft 365 data, and apply Azure delete locks and soft delete where the district hosts workloads.
- Test paper-based procedures and how buildings operate when phones, cameras, and door systems are down; pre-select a vetted incident response firm and know your insurer and law enforcement contacts.

LTC vCISO Program

The vCISO Program provides K-12 school districts with affordable, shared, senior-level cybersecurity leadership, risk guidance, and strategic decision support without the high cost of hiring a full-time Chief Information Security Officer.

This monthly report is compiled by the vCISO program from research and observations. It is used in the service of the vCISO program's direct work with partner districts, but is also shared with the broader community. If you are interested in engaging the vCISO program to apply this data directly to your district's needs, please contact the LTC.

References

K–12 District Incidents

- https://www.securitymagazine.com/articles/102596–spokane-public-schools-faces-cybersecurity-incident
- https://www.spokesman.com/stories/2026/oct/08/spokane-public-schools-suspects-student-staff-data/
- https://www.govtech.com/education/k-12/spokane-schools-cyber-attack-may-have-compromised-data
- https://cybernews.com/news/school-district-ransomware-attack-idaho-cameras-locks-hvac/
- https://www.eastidahonews.com/2026/10/cybersecurity-incident-forced-jerome-schools-to-close-monday-district-says-student-data-is-safe/
- https://thereminder.com/local-news/easthampton-public-schools-suffers-cyberattack/
- https://dysruptionhub.com/indiana-area-district-cyber-incident/
- https://www.wccsradio.com/2026/10/16/indiana-school-district-continues-to-deal-with-fallout-of-cyberattack/
- https://dysruptionhub.com/north-slope-alaska-cyber-incident-recovery/
- https://dysruptionhub.com/incidents/profiles/lakin-unified-school-district-215–2026–01/
- https://hoodline.com/2026/10/rural-wisconsin-school-district-loses-92–000–in-cyberattack-manager-put-on-leave/
- https://www.wpr.org/news/cybercrime-attacks-on-wisconsin-schools
- https://www.dapeer.com/databreaches/alisal-union-school-district-data-breach-investigation
- https://oag.ca.gov/privacy/databreach/list
- https://www.galaxywarden.com/blog/breach/tulare-western-high-school-boobaproject-2026–09
- https://www.board-cybersecurity.com/incidents/tracker/tulare-joint-union-high-school-district-cybersecurity-incident-27c65ef4
- https://www.board-cybersecurity.com/incidents/tracker/inner-city-education-foundation-cybersecurity-incident-0e9a3b74
- https://dysruptionhub.com/slate-valley-vermont-ransom-demand/
- https://www.ransomware.live/id/Sm9saWV0IFB1YmxpYyBTY2hvb2xzIERpc3RyaWN0IDg2QHFpbGlu

- https://ransomware.live/id/Q2hhbXBhaWduIFVuaXQgNCBTY2hvb2wgRGlzdHJpY3RAVllQUg==
- https://www.ransomware.live/id/TGxhbm8gSW5kZXBlbmRlbnQgU2Nob29sIERpc3RyaWN0QHFpbGlu
- https://www.ransomware.live/id/U2VtaW5vbGUgU2Nob29sc0BHbG9iYWwgU2VjcmV0IEdyb3Vw
- https://www.ransomware.live/id/QW5zb25pYSBQdWJsaWMgU2Nob29sc0B0aGVnZW50bGVtZW4=
- https://ransomware.live/id/U2FudGVllFNjaG9vbCBEaXN0cmljdCBGb3VuZGF0aW9uQHRoZWdlbnRsZW1lbg==
- https://ransomware.live/id/VGhlIE5ldyBDb21tdW5pdHkgU2Nob29sQGluY3JhbnNvbQ==
- https://www.ransomware.live/id/RnJpZW5kc2hpcCBDaHJpc3RpYW4gU2Nob29sQHFpbGlu
- https://ransomware.live/id/U2xhdGUgVmFsbGV5IFVuaWZpZWQgU2Nob29sIERpc3RyaWN0QGthaXJvcw==
- https://dysruptionhub.com/south-carolina-voucher-phishing-payments/
- https://dysruptionhub.com/incidents/profiles/maryland-state-department-of-education-2026-01/
- https://hoodline.com/2026/10/cyberattack-knocks-out-phones-email-at-53-richmond-public-schools/
- https://tech-insider.org/ransomware-data-theft-surge-schools-hospitals-2026/
- https://dailynorthwestern.com/2026/10/14/lateststories/eths-faces-uphill-battle-following-june-ransomware-attack/

Vendor Breaches (Frontline, ETS)

- https://www.bleepingcomputer.com/news/security/frontline-education-data-breach-impacts-school-district-employees/
- https://www.infosecurity-magazine.com/news/frontline-education-breach-k12/
- https://txlrs.org/blog-post/texas-frontline-education-school-employee-data-breach-october-2026
- https://www.herecolumbia.com/2026/10/08/frontline-education-data-breach-sc-school-districts/
- https://fpsct.org/district-departments/technology-services/frontline-education-data-breach/
- https://www.board-cybersecurity.com/incidents/tracker/kern-county-superintendent-of-schools-cybersecurity-incident-219b8df5

- https://www.latimes.com/california/story/2026-10-16/state-testing-student-data-hack
- https://www.cde.ca.gov/nr/ne/yr26/yr26rel45.asp
- https://www.edweek.org/technology/hackers-steal-personal-data-of-millions-of-california-students-in-massive-breach/2026/10
- https://www.cbsnews.com/sanfrancisco/news/california-state-testing-ets-data-breach-impact-millions-of-students-officials-say/
- https://whiteboardadvisors.com/cybersecurity-breaches-are-the-new-normal-for-k-12/
- https://www.prnewswire.com/news-releases/new-report-finds-one-in-two-us-school-districts-experienced-a-cybersecurity-incident-in-2025-302709821.html

Vulnerabilities and Patching

- https://thehackernews.com/2026/09/warning-two-unpatched-citrix-netscaler.html
- https://therecord.media/us-australia-warn-of-latest-citrix-vulnerability
- https://www.rapid7.com/blog/post/etr-zero-day-exploitation-of-citrix-netscaler-adc-and-gateway-cve-2026-88771-and-cve-2026-88772/
- https://www.helpnetsecurity.com/2026/10/05/cisa-flags-new-exploited-netscaler-flaw-as-attackers-crash-appliances-cve-2026-88779/
- https://support.citrix.com/external/article/CTX697096/citrix-netscaler-adc-and-citrix-netscale.html
- https://cyberscoop.com/microsoft-patch-tuesday-october-2026/
- https://securityaffairs.com/200965/hacking/u-s-cisa-adds-microsoft-windows-shell-flaw-to-its-known-exploited-vulnerabilities-catalog.html
- https://www.securityweek.com/microsoft-sharepoint-flaw-cve-2026-65660-now-exploited-in-attacks/
- https://thehackernews.com/2026/09/sharepoint-flaw-initially-listed-as.html
- https://therecord.media/warlock-ransomware-used-in-critical-infrastructure-attacks
- https://www.security.com/threat-intelligence/warlock-ransomware-critical-infrastructure
- https://thehackernews.com/2026/10/microsoft-exchange-flaw-lets.html
- https://www.helpnetsecurity.com/2026/10/05/exchange-server-vulnerability-cve-2026-96940/
- https://www.bleepingcomputer.com/news/microsoft/microsoft-windows-server-2022-reached-end-of-mainstream-support/
- https://www.bleepingcomputer.com/news/security/cisco-warns-of-new-sd-wan-authentication-bypass-zero-day-exploited-in-attacks/
- https://thehackernews.com/2026/10/cisa-adds-exploited-cisco-catalyst-sd.html

- https://www.bleepingcomputer.com/news/security/cisco-warns-of-critical-flaws-allowing-nexus-switch-takeover/
- https://thehackernews.com/2026/10/critical-sonicwall-sma-1000-flaw.html
- https://www.helpnetsecurity.com/2026/10/07/sonicwall-fixes-pre-auth-ssrf-flaw-in-sma-1000-appliances-cve-2026-102255/
- https://www.bleepingcomputer.com/news/security/apple-patches-coregraphics-zero-day-flaw-exploited-in-attacks/
- https://thehackernews.com/2026/10/apple-coregraphics-poc-emerges-as.html
- https://www.bleepingcomputer.com/news/security/hackers-start-exploiting-critical-wordpress-flaw-for-code-execution/
- https://www.helpnetsecurity.com/2026/09/23/cve-2026-87902-wordpress-7-1-2-security-release/
- https://www.bleepingcomputer.com/news/security/drupal-patches-critical-rce-flaws-warns-exploits-may-emerge-soon/
- https://www.drupal.org/sa-core-2026-014
- https://thehackernews.com/2026/10/libreoffice-and-openoffice-flaws-let.html
- https://securityaffairs.com/200734/security/u-s-cisa-adds-proftpd-onlyoffice-docs-strapi-apache-struts-and-isc-bind-flaws-to-its-known-exploited-vulnerabilities-catalog.html
- https://www.securityweek.com/adobe-patches-140-vulnerabilities-across-10-products/

Identity, Cloud, and Third-Party Access

- https://thehackernews.com/2026/10/connectwise-suspends-cloud-backup-after.html
- https://thehackernews.com/2026/10/connectwise-resets-credentials-as-cloud.html
- https://www.cybersecuritydive.com/news/connecwise-suspends-cloud-backup-hacker-microsoft-365/833345/
- https://www.securityweek.com/meta-says-hackers-took-code-personal-data-of-1500-in-github-breach/
- https://www.bleepingcomputer.com/news/security/jadepuffer-agentic-ai-attacks-target-azure-destroy-cloud-resources/
- https://thehackernews.com/2026/10/wazza-phishkit-targets-banking.html
- https://www.levelblue.com/blogs/spiderlabs-blog/inside-wazza-a-newly-observed-device-code-phishing-kit-targeting-microsoft-365-accounts
- https://www.theguardian.com/money/2026/oct/11/calendar-phishing-scam-meeting-renewal-google-microsoft-paypal

- https://www.securityweek.com/astrana-health-data-breach-impacts-private-confidential-information/
- https://www.bleepingcomputer.com/news/security/hackers-breach-pentagon-human-resources-management-system-steal-data-of-nearly-3-million-people/

Malware, Evasion, and AI

- https://www.securityweek.com/fake-lastpass-installers-push-kernel-level-edr-killer-rapuncel-stealer/
- https://www.bleepingcomputer.com/news/security/fake-lastpass-authenticator-github-repos-push-new-rapuncel-infostealer/
- https://thehackernews.com/2026/09/attackers-abuse-chatgpt-custom-gpts-to.html
- https://thehackernews.com/2026/09/taskstomp-powershell-backdoor-steals.html
- https://www.securityweek.com/nightmare-eclipse-drops-new-microsoft-defender-exploit-after-revealing-identity/
- https://www.wired.com/story/a-tool-for-tracking-ai-integrated-malware-uncovered-an-autonomous-command-system/
- https://blog.talosintelligence.com/the-closed-quorum-inside-the-first-reported-autonomous-ai-c2-implant/
- https://www.bleepingcomputer.com/news/security/automated-ai-agent-used-to-breach-cybersecurity-nonprofit-divd/
- https://www.bleepingcomputer.com/news/security/divd-says-zammad-zero-days-enabled-ai-driven-network-breach/
- https://cyberscoop.com/poellm-malware-botnet-poem-lumen-black-lotus-labs/
- https://therecord.media/ai-set-to-help-attackers-more-than-defenders
- https://www.securityweek.com/enterprises-struggle-to-prepare-for-ai-and-quantum-threats-pwc-says/
- https://www.securityweek.com/supermarket-refrigeration-attack-widens-to-copeland-dixell-controllers/

Law Enforcement and Industry

- https://www.cnn.com/2026/10/09/politics/fbi-arrest-shinyhunters-hack
- https://www.bleepingcomputer.com/news/security/fbi-arrests-another-suspected-shinyhunters-hacker-after-agency-breach/
- https://www.reuters.com/technology/accenture-contractor-removed-fbi-following-damaging-data-breach-sources-say-2026-10-06/

- https://cloud.google.com/blog/topics/threat-intelligence/shinyhunters-targets-education-sector-oracle-exploit
- https://cyberscoop.com/killsec-ransomware-group-arrests-operation-killswitch/
- https://therecord.media/ransomware-recovery-charges-doj
- https://www.bleepingcomputer.com/news/security/microsoft-teams-will-let-admins-block-custom-file-extensions/
- https://www.bleepingcomputer.com/news/microsoft/microsoft-outlook-to-block-msix-attachments-used-in-attacks/
- https://www.infosecurity-magazine.com/news/attackers-hijack-cctlds-obtain/
- https://www.darkreading.com/cloud-security/cloudflare-announces-public-certificate-authority-post-quantum-web
- https://www.securityweek.com/google-partially-reverses-chrome-bug-bounty-cuts/
- https://www.forbes.com/sites/gradsoflife/2026/10/15/closing-the-cybersecurity-gap-why-teachers-cant-be-on-the-sidelines/

Executive Summary

This month, the biggest risks to schools came through their vendors. A stolen password at California's state testing company exposed information on millions of students, including disability status and test scores. A breach at Frontline Education, a common school HR software provider, exposed staff Social Security numbers in several states. A backup company used by many IT providers had its access to customer Microsoft 365 accounts misused.

At least 18 schools and districts nationwide were attacked or named by ransomware gangs. An Idaho district closed for two days after attackers reached cameras, door locks, and heating systems. Criminals also kept breaking into remote-access equipment before fixes were available and are now using artificial intelligence to move faster.

The lesson for leadership: ask vendors hard questions about how they protect student and staff data, require stronger sign-in protections, install urgent security updates within days, and plan to run the school safely when technology fails.