



**Learning
Technology
Center**

vCISO PROGRAM

Monthly Cyber Threat Intelligence

August 2026

Compiled by Learning Technology Center, vCISO Program

Covers July 20, 2026 through August 19, 2026

Table of Contents

Table of Contents	2
Introduction	3
Threat Landscape for August 2026	3
Monthly Areas of Focus	3
Critical macOS Screen Sharing Authentication Bypass — Active Exploitation (CVE-2026-65400)	4
MacSync Infostealer — Rotating C2 Domain Infrastructure Targeting State/Local Government	4
"WP2Shell" — Unauthenticated Remote Code Execution in WordPress Core (CVE-2026-63030 / CVE-2026-60137)	5
Over 24,000 Internet-Exposed Server BMCs Leak Password Hashes via a 22-Year-Old Flaw	5
SAP Commerce Cloud Critical RCE (CVE-2026-58231) — Exploited Days After Patch	6
Azure/Entra Credential Theft Campaign Exposes Millions of Fortune 500 Employee Records	6
ChainDrop — Self-Propagating npm Supply Chain Worm Infects 400+ Packages	7
New TrickBot Variant Uses DNS Tunneling for Command-and-Control	8
Recommendations	8
Identity and access	8
Network architecture.	8
Incident response and continuity planning.	8
Awareness and training.	9
LTC vCISO Program	9
K-12 Breach Sources (district incidents):	9
References	9
Executive Summary	10

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 August 2026 reporting period is defined by a shift toward pervasive credential theft and supply chain vulnerabilities, where attackers are leveraging stolen passwords and vendor dependencies rather than complex new exploits. As the back-to-school season begins, this landscape underscores the critical need for phishing-resistant MFA and rigorous vendor scrutiny to protect core district infrastructure.

Threat Landscape for August 2026

August's activity kept circling back to one theme: attackers are getting in through stolen passwords and legitimate-looking prompts, not sophisticated new exploits, and the platforms and vendors districts depend on are just as exposed as the districts themselves. Credential theft was the headline risk, highlighted by a campaign that exfiltrated roughly 3.5 to 4.8 million employee records from Microsoft Entra ID tenants at several large organizations, a reminder that MFA needs to be mandatory and phishing-resistant, not just a checkbox.

macOS also moved further into attackers' sights this month. A ClickFix campaign tied to more than 30 rotating command and control domains is actively compromising Mac devices, and a separate authentication bypass in macOS Screen Sharing (CVE-2026-65400) shows that the days of treating Apple hardware as a lower priority target are over, especially in classrooms where student and staff devices often share the same network.

Malware is also getting harder to spot, with a new TrickBot variant hiding its command-and-control (C2) traffic inside routine DNS queries, right where most content filters are not looking. Supply chain exposure grew too, with the ChainDrop worm spreading through more than 400 npm packages and a critical, plugin-free remote code execution chain in core WordPress, known as wp2shell, putting district and vendor websites at risk.

All of this lands during the back-to-school window, the same stretch of the calendar that forced Newton County, GA and Sumner County, TN to delay or shut down school after cyber incidents last year. That timing is the real takeaway for August. Strong MFA, a tested incident response plan, and real scrutiny of vendor security are not optional right now; they are the difference between a normal opening week and a headline.

Monthly Areas of Focus

Critical macOS Screen Sharing Authentication Bypass — Active Exploitation (CVE-2026-65400)

Severity: Medium

What happened: A vulnerability in the built-in macOS Screen Sharing service allows a remote attacker to bypass authentication and gain root access on local and directly attached, internet-exposed Macs. While it is very unlikely that a Mac is directly connected to the internet with a public IP address, a full ItoI port forwarding would allow this attack. The more common focus of this attack would be local line-of-sight WiFi and Bluetooth connectivity.

K-12 relevance: Many schools leverage MacBook Airs and Pros for teacher devices and Neos and Airs for some students. In close proximity and in networks with little or no segmentation between students' and staff devices, this vulnerability can be widely used in classrooms this fall. While root access can lead to devastating incidents and perhaps a breach, the more common attack surface will take the form of classroom distractions and pranks.

Recommended action: A layered network architecture would provide some mitigation to this issue. Network segmentation and WiFi client isolation will force this attack into the more difficult and up-close Bluetooth attack surface. Additionally, this issue reinforces the need for a consistent, proactive process to keep macOS up to date with the latest version, and for a method and organizational culture that enable end devices to be updated and patched quickly.

MacSync Infostealer — Rotating C2 Domain Infrastructure Targeting State/Local Government

Severity: Medium

What happened: In the July CTI, it was reported that a social engineering technique called “ClickFix” was being implemented. A quick refresher: “ClickFix” is a fake CAPTCHA/verification page or an AI tool installer that tricks users into running code or scripts. Last month's article focused heavily on PowerShell and Python scripts.

This month, Microsoft's threat intelligence team reported identifying 30+ command-and-control (C2) servers actively leveraging ClickFix to compromise macOS devices. CIS/MS-ISAC has confirmed Microsoft's findings through documented activity from their MDBR service that blocks DNS queries to known C2 or other malicious servers.

K-12 relevance: macOS is widely used in K-12 education. Your users are hit daily with CAPTCHAs or human verification pages. This attack surface can be successful in organizations without layered security such as MDBR or an EDR/MDR client on the Mac device. The days of seeing the Mac as a lower-level target or a security-by-obscurity approach are over.

Recommended action: Mac-heavy districts will need to move forward and follow the path of Microsoft device-heavy districts. They need to start building a layered cybersecurity plan,

including endpoint detection and response (EDR) and network tools like MDBR, as well as log ingestion tools such as a SIEM.

"WP2Shell" — Unauthenticated Remote Code Execution in WordPress Core (CVE-2026-63030 / CVE-2026-60137)

Severity: High

What happened: Researchers disclosed a two-flaw exploit chain ("wp2shell") affecting default WordPress core installations, requiring no plugins, described as the first critical unauthenticated WordPress core RCE in nearly a decade. Chaining a REST API request-confusion bug with a SQL injection lets an unauthenticated attacker achieve full site takeover, and it is now being exploited broadly and opportunistically.

K-12 relevance: High for public-facing web presence. Many districts, PTAs, booster clubs, alumni associations, and small ed-tech vendors run WordPress, often on shared hosting with irregular patch cadence. This is exactly the profile of opportunistic, mass-scanned targets this flaw favors. No plugin is required, so even minimal default sites are exposed.

Recommended action: Open-source software is not free. The use of open-source software transfers responsibility and management to the IT staff. This fact should be accounted for in IT staffing levels and time commitments. As long as staff, skills, and maintenance time are managed well, open-source software is a very economical alternative. If a district or a department leverages an open-source package for production and does not account for these factors—utilizing a “set it and forget it” model this attack surface is the result. Ownership, knowledge, and skill in the main package and the underlying operating system are prerequisites for utilizing WordPress or other open-source assets.

Over 24,000 Internet-Exposed Server BMCs Leak Password Hashes via a 22-Year-Old Flaw

Severity: Medium

What happened: Security firm Lava scanned the internet and found roughly 36,872 exposed IPMI (server remote-management) services, of which 24,650 disclosed password-derived authentication hashes before any login attempt. The root cause is CVE-2013-4786, a long-known weakness in the IPMI 2.0 / RMCP+ authentication protocol. Over 30% of recovered hashes matched common wordlists, and default passwords for HPE iLO and Supermicro management chips were crackable in minutes.

K-12 relevance: Districts running on-prem data centers for SIS, ERP, or finance systems often use rack servers (Dell, HPE, Supermicro) with Baseboard Management Controllers (BMCs) enabled by default. Exposure typically results from limited network segmentation or from misconfigured port

forwarding by smaller IT shops or MSPs. Successful compromise grants remote console/OS-independent control, potentially bypassing endpoint protections entirely.

Recommended action: Remote management is a necessity for K12 technology departments. Professionals leverage remote access to improve work-life balance, create more flexible maintenance windows, and address emergencies. Remote access also allows districts to do more with less staff. Remote access is only as secure as the weakest link in authentication. Remote ports should not be mapped directly to public addresses.

All remote management should be on a limited-access virtual local area network (VLAN) segment. This engineering design prevents both internal and external endpoints from directly accessing the service. The segmented VLAN should be accessed only by a virtual private network (VPN) with two-factor authentication or a highly regulated internal network (wired or wireless).

SAP Commerce Cloud Critical RCE (CVE-2026-58231) — Exploited Days After Patch

Severity: Low

What happened: SAP disclosed a maximum-severity (CVSS 10.0) flaw in SAP Commerce Cloud's Data Hub Adapter extension, allowing an unauthenticated attacker to execute code remotely via a default authentication client and unvalidated input functions. Exploitation attempts began just three days after the patch, before a public proof of concept existed.

K-12 relevance: Low direct risk, but a real vendor/supply-chain exposure. School districts do not run SAP Commerce Cloud directly, but online payment processors, school-store/spirit-wear vendors, and nutrition-services procurement platforms sometimes run on it. A vendor compromise during back-to-school procurement season could disrupt payments or expose payment data.

Recommended action: Districts should work with their vendors to document that said vendor has applied Note 3771065. Districts should not hesitate to engage with vendors regarding their cybersecurity processes. School Districts should leverage tools to determine the major software their vendors are using. Districts can then use their vendor's data to actively engage in a complete cybersecurity process. One free tool is Educause's Higher Education Community Vendor Assessment Toolkit (HECVAT).

Azure/Entra Credential Theft Campaign Exposes Millions of Fortune 500 Employee Records

Severity: High

What happened: A threat actor using the alias "TheHatman" is selling internal directory data allegedly taken directly from the Microsoft Entra ID (Azure AD) tenants of at least nine large organizations, including McDonald's, Vodafone, TCS, and others. Roughly 3.5–4.8 million employee records were exposed. This was not a breach of the Azure platform itself but a compromise of individual customer tenants, most likely via stolen credentials, infostealer malware, or password-spray/MFA-fatigue attacks.

K–12 relevance: High. Districts overwhelmingly run Microsoft 365/Entra ID for staff and student accounts and store FERPA-protected records in Azure/SharePoint/OneDrive. This incident illustrates the dominant real-world risk pattern for schools: weak MFA enforcement, credential/infostealer compromise, and over-permissioned third-party ed-tech app integrations connected via Entra.

Recommended action: This incident reinforces that credential stealing and compromise are a larger threat than zero-days. School leaders need to know that MFA as a check box is no longer sufficient. Schools need to enforce phishing-resistant MFA (FIDO2/passkeys) for all staff, especially IT/admin accounts; audit and minimize third-party app permissions in Entra ID; deploy conditional access policies; and run periodic cloud misconfiguration scans on tenants that store student data. Finally, continue refining staff training on the proper use of authentication techniques.

ChainDrop — Self-Propagating npm Supply Chain Worm Infects 400+ Packages

Severity: Medium

What happened: A self-propagating worm dubbed "ChainDrop" (also called "Mini Shai-Hulud") compromised over 400 npm JavaScript packages — some reports later put the total over 1,300 — after attackers gained access to a maintainer's GitHub account and used stolen npm publishing tokens to automatically infect and republish other packages. Affected packages include widely used utilities such as keyv, flat-cache, cache-manager, and file-entry-cache, which are embedded deep within many organizations' software supply chains.

K–12 relevance: Districts rarely maintain npm packages themselves, but many rely on vendor-built web portals, LMS integrations, or in-house developer tools built on Node.js — any of which could pull in a compromised dependency during a routine npm install. The credential-harvesting payload specifically targets CI/CD and cloud credentials, which is the same class of access used to manage hosted district systems.

While school districts are not developers, those that deploy open-source software need to take on some developer-level oversight. Leveraging open source has price benefits but transfers that cost to employee and institutional skill.

Recommended action: Schools that leverage in-house developers or use open-source software will need to implement controls to address such supply chain attacks. This attack surface has increased in the past 3 years and is expected to continue. The open-source and developer

communities leverage these packages, creating a domino effect. It takes only one compromised susceptible package to lead to a devastating incident.

New TrickBot Variant Uses DNS Tunneling for Command-and-Control

Severity: High

What happened: FortiGuard Labs identified a TrickBot variant that abandons the malware's historical HTTP-based command-and-control in favor of DNS tunneling. TrickBot is encoding commands inside DNS queries and responses to evade network-based detection. The variant retains TrickBot's modular architecture (module downloads, process injection, PowerShell/shellcode execution).

K-12 relevance: Many district networks forward DNS to upstream resolvers without deep inspection, and standard web-content filters used for CIPA compliance inspect HTTP/HTTPS traffic but rarely analyze DNS query patterns closely. As a modular loader, a successful foothold can quickly escalate to ransomware deployment against student information systems, payroll, and other critical infrastructure.

Recommended action: Route all internal DNS through monitored resolvers and block direct outbound DNS to arbitrary external servers; deploy DNS tunneling/anomaly detection; audit Task Scheduler for obfuscated entries; maintain behavioral EDR, not just signature-based antivirus; reinforce phishing awareness training, including TrickBot's typical delivery methods.

Recommendations

Identity and access

Require phishing-resistant multi-factor authentication (FIDO2/passkeys or, at minimum, app-based MFA) for all staff accounts, with no exceptions for administrative or service accounts. Enforce conditional access policies that flag impossible-travel logins, unmanaged devices, and password-spray patterns. Regularly review and prune Entra ID / Google Workspace third-party app permissions, since over-permissioned ed-tech integrations were a recurring theme this month.

Network architecture.

Segment IoT devices, security cameras, and BMC/management interfaces onto isolated VLANs with restricted outbound internet access. Route DNS through monitored, controlled resolvers and consider DNS tunneling/anomaly detection, given this month's TrickBot findings.

Incident response and continuity planning.

Conduct or update a tabletop exercise before the start of the school year specifically simulating a pre-opening network shutdown, modeled on the Newton County and Sumner County incidents,

including paper-based fallback procedures, board and family communication templates, and law-enforcement coordination steps.

Awareness and training.

Brief technology staff specifically on ClickFix-style social engineering (fake "paste this command" prompts) and thread-hijacking phishing that originates from real, previously compromised contacts, both of which are notable this month for successfully targeting experienced technical staff, not just general users.

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.

K-12 Breach Sources (district incidents):

- Newton County Schools, Covington, GA
- School districts in Vermont (phishing attack)
- District of Columbia Public Schools
- Sumner County Schools, Gallatin, TN

References

- <https://arstechnica.com/security/2026/08/vulnerability-giving-attackers-full-control-of-macs-is-under-active-exploitation/>
- <https://thehackernews.com/2026/08/microsoft-links-30-rotating-domains-to.html>
- <https://thehackernews.com/2026/07/new-wp2shell-wordpress-core-flaw-lets.html>
- <https://www.bleepingcomputer.com/news/security/over-24-000-exposed-server-bmcs-leak-password-hash-via-decades-old-flaw/>
- <https://thehackernews.com/2026/08/sap-commerce-cloud-cve-2026-58231.html>
- <https://www.helpnetsecurity.com/2026/08/18/azure-data-leak-fortune-500-companies/>

- <https://www.securityweek.com/over-400-npm-packages-infected-in-chaindrop-supply-chain-attack/>
- <https://www.fortinet.com/blog/threat-research/inside-a-trickbot-variant-using-dns-tunneling-for-c2>
- <https://techcrunch.com/2026/08/05/psa-apples-private-relay-can-leak-your-real-ip-address/>

Executive Summary

This month, attackers mostly succeeded by stealing passwords and login credentials, and outside vendors, apps, and devices posed as much risk as anything districts control directly. Two districts in Georgia and Tennessee had to shut down or delay the start of school after cyber incidents in the days just before classes began, showing that back-to-school week is a known high-risk period.

The lesson for leadership: firewalls alone won't protect a district if passwords are weak, vendor tools go unchecked, and management system devices can be reached from everywhere. This fall, districts should focus on three things: require strong multi-factor authentication for all staff, with no exceptions; run a practice drill for a network shutdown before school starts; and verify that key vendors are actually secure, rather than assuming they are. Taking these steps now, before the riskiest weeks of the year, is the best way to avoid being next month's headline.