



Daily Cyber Headlines

Daily Cyber
Headlines

☐ TLP:WHITE

Alert ID :
8809d2ec

Oct 05, 2026, 05:07
AM



Today's Headlines:

Leading Story

- Citrix Patches NetScaler SAML Zero-Day Exploited in Attacks

Data Breaches & Data Leaks

- Data Breaches Announced by Saber Healthcare & Buchalter

Cyber Crimes & Incidents

- China-Aligned TA419 Targets U.S. AI Policy Experts With Microsoft AitM Phishing
- Warlock Exploits SharePoint Flaws to Disable Security Tools and Deploy Ransomware

Vulnerabilities & Exploits

- Fortra Patches Critical Vulnerabilities in BoKS
- Dell Asks Admins to Patch Max Severity CSM Flaws As Soon As Possible

Trends & Reports

- Broadband Gaps Leave Rural Communities Facing Multiple Barriers To Care

Privacy, Legal & Regulatory

- Nothing to Report

Upcoming Health-ISAC Events

- Global Monthly Threat Brief
 - Americas – October 27, 2026, 12:00 PM - 1:00 PM ET
 - European – October 28, 2026, 03:00-04:00 PM CET
 - APAC – October 30, 2026, 01:00-02:00 PM AEST

Additional Information

Leading Story

Citrix Patches NetScaler SAML Zero-Day Exploited in Attacks

Summary

- Citrix issued patches for a NetScaler SAML vulnerability that has been actively targeted in attacks, causing service disruptions.

Analysis & Action

Citrix released updates for CVE-2026-88779, a NetScaler memory buffer vulnerability affecting SAML authentication, that attackers actively exploit to disrupt availability and potentially enable arbitrary code execution. For more information, Health-ISAC [published](#) an advisory for this.

Healthcare networks that rely on NetScaler for secure remote access are vulnerable to service outages or unauthorized access, endangering electronic health record availability, clinical workflows, patient care delivery, and data privacy.

Health-ISAC advises its members to immediately apply Citrix emergency updates, implement recommended global IP deny lists, review SAML configurations, and monitor system logs for suspicious device reboot activity.

Data Breaches & Data Leaks

Data Breaches Announced by Saber Healthcare & Buchalter

Summary

- Saber Healthcare, an Ohio-based care provider, and Buchalter LLP, a law firm serving Arrowhead Regional Medical Center in California, have recently disclosed data security incidents involving unauthorized access to their servers, compromising sensitive personal and medical data.

Analysis & Action

Saber Healthcare identified unauthorized server access on July 27, 2026, which exposed a range of sensitive data including health information, financial account details, and Social Security numbers, affecting over 3,000 individuals. Similarly, Buchalter LLP discovered on August 28, 2026, that an unauthorized third party accessed limited data sets provided to them by Arrowhead Regional Medical Center for legal services. Both organizations engaged third-party cybersecurity experts to investigate the scope of the breaches and mitigate further unauthorized activity.

Organizations involved in managing or handling protected health information must enforce stringent network security measures and routinely audit data security policies. Health-ISAC advises its members to implement phishing-resistant authentication mechanisms, such as FIDO2 passkeys or hardware security keys, for critical enterprise identities. Those potentially impacted are advised to monitor their financial accounts, credit reports, and health insurance statements closely to guard against identity theft and fraud. Healthcare entities should ensure continuous evaluation of both internal systems and the security practices of third-party vendors and business associates.

Cyber Crimes & Incidents

China-Aligned TA419 Targets U.S. AI Policy Experts With Microsoft AitM Phishing

Summary

- China-aligned threat group TA419 targeted U.S. AI policy experts at think tanks and universities using adversary-in-the-middle phishing. Attackers impersonated high-profile individuals to deploy custom BitB frameworks and harvest Microsoft credentials without user detection.

Analysis & Action

A China-nexus cyber-espionage actor tracked as TA419 has been conducting credential-phishing campaigns against artificial intelligence policy experts in the United States. Active since at least April 2025, the threat group primarily targets think tanks, higher education institutions, legal organizations, and defense contractors. Recent operations impersonated prominent figures, including a former White House science

advisor and an Anthropic employee, establishing rapport via initial social-engineering emails before sending malicious lures disguised as feedback requests.

The phishing sequence leverages multi-stage redirection chains routed through Cloudflare Turnstile to reach adversary-in-the-middle proxy infrastructure hosted on OneDrive. TA419 uses a Frameless Browser-in-the-Browser technique that combines HTML, CSS, and JavaScript substitutions, without standard iframes, to mimic valid sign-in interfaces. Enhanced with custom telemetry and automation modules, the proxy relays authentic authentication flows to legitimate Microsoft servers while stealthily capturing session cookies and credentials, effectively bypassing standard multi-factor authentication.

Health-ISAC advises its members to implement phishing-resistant authentication mechanisms, such as FIDO2 passkeys or hardware security keys, for critical enterprise identities. Security teams should conduct threat hunting for anomalous redirect flows involving Cloudflare Turnstile and unexpected external proxy connections during Microsoft authentication. Additionally, organizations should educate research, legal, and policy staff to independently verify unsolicited subject-matter outreach before engaging with links or executing sign-in requests.

Warlock Exploits SharePoint Flaws to Disable Security Tools and Deploy Ransomware

Summary

- Threat group Warlock actively exploits Microsoft SharePoint vulnerabilities to compromise organizations across critical infrastructure and government. The actor deploys web shells, disarms Endpoint Detection and Response tools via vulnerable drivers, and stages ransomware through Active Directory shares.

Analysis & Action

The suspected China-linked threat actor known as Warlock, also tracked as Gold Salem, Longlegs, and Storm 2603, is actively exploiting unpatched Microsoft SharePoint vulnerabilities to conduct ransomware attacks. Recent activity observed by Symantec and Carbon Black targeted critical infrastructure, government bodies, and educational institutions in Portuguese- and Spanish-speaking regions across Europe, Africa, and Latin America. Warlock leverages web shell drops on exposed SharePoint servers as an initial access vector to maintain long-term persistence within targeted enterprise environments.

Technically, attackers drop web shells to extract ASP.NET machine keys from compromised SharePoint farms, enabling them to forge validly signed payloads that

execute arbitrary code within the SharePoint application pool. To disarm endpoint protections, Warlock executes Bring Your Own Vulnerable Driver attacks using a vulnerable driver (CVE-2025-1055) to terminate security tools across dozens of network hosts within hours. The group subsequently establishes remote access via Microsoft Visual Studio Code tunnels and stages ransomware binaries within the domain's SYSVOL shares for rapid domain-wide distribution.

Health-ISAC advises its members to immediately apply all security updates for on-premises Microsoft SharePoint Server installations and audit SharePoint farms for unauthorized web shells or modified ASP.NET machine keys. Organizations should implement Driver Blocklists to mitigate Bring Your Own Vulnerable Driver attacks and monitor endpoints for the unauthorized execution of vulnerable drivers, such as K7RKScan.sys. Furthermore, security operations teams should restrict outbound connectivity for administrative developer utilities, audit Active Directory SYSVOL shares for unauthorized binary staging, and monitor for unauthorized Visual Studio Code tunnel usage.

Vulnerabilities & Exploits

Fortra Patches Critical Vulnerabilities in BoKS

Summary

- Fortra released security updates patching eight vulnerabilities in Core Privileged Access Manager (BoKS), including three critical flaws. Exploitation could allow remote attackers to achieve authentication bypass, root command execution, and system memory corruption across Unix and Linux management infrastructure.

Analysis & Action

Fortra has issued security patches addressing eight vulnerabilities in its Core Privileged Access Manager (BoKS), software commonly deployed to centrally enforce access policies across enterprise Unix and Linux environments. The update fixes three critical-severity flaws alongside five high- and medium-severity vulnerabilities. Fortra noted that BoKS Manager deployments that use the BoKS keytab for Active Directory service account management are exposed to key-generation weaknesses, though no active exploitation in the wild has been observed to date. For more information, Health-ISAC [published](#) an advisory for this.

Technically, the most severe flaw (CVE-2026-79901, CVSS 9.9) stems from predictable pseudo-random sequence seeding using Unix timestamps, enabling authenticated Active Directory users to offline-verify and reproduce candidate passwords for targeted service accounts. Additionally, CVE-2026-79898 (CVSS 9.1) allows authenticated attackers to execute shell commands as root on the BoKS Master via the crlserver REST or SOAP APIs, without requiring local escalation privileges. A third critical bug, CVE-2026-12627 (CVSS 9.8), manifests as a stack buffer overflow in the autoregistration function, enabling remote memory corruption.

Health-ISAC advises its members to prioritize upgrading Fortra Core Privileged Access Manager (BoKS) installations to the latest patched version to remediate these critical vulnerabilities. Organizations that use BoKS keytabs for Active Directory integration should review service account password reset workflows and audit Kerberos ticket requests for anomalous activity. Furthermore, security teams should restrict network access to BoKS WSI REST and SOAP APIs, enforcing strict network segmentation and least-privilege access controls across Unix and Linux management fleets.

Dell Asks Admins to Patch Max Severity CSM Flaws As Soon As Possible

Summary

- Dell released updates for Container Storage Modules to fix authorization vulnerabilities that could allow unauthorized administrative access to storage infrastructure.

Analysis & Action

Dell patched vulnerabilities in Container Storage Modules, which integrate storage arrays with Kubernetes. These flaws allow unauthorized users to gain administrative control over storage infrastructure. For more information, Health-ISAC [published](#) an advisory for this.

In the health sector, compromised storage systems could expose patient records, disrupt clinical operations, or alter medical data. Attackers could exploit authentication gaps to bypass access controls on enterprise databases

Health-ISAC advises its members to apply Dell's CSM version 1.18.0 update immediately, review network exposure of storage interfaces, and restrict access to authorized Kubernetes cluster management systems.

Trends & Reports

Broadband Gaps Leave Rural Communities Facing Multiple Barriers To Care

Summary

- Nearly 12 million people across 41 states live in areas with inadequate broadband, limiting telehealth's potential to reach communities where healthcare is already difficult to access.

Analysis & Action

Researchers classified areas as broadband deserts when speed fell below 100 megabits per second (Mbps) for downloads and 20 Mbps for uploads. Of the estimated 12 million in broadband deserts, 10.5 million, or 88%, lived in rural areas.

Findings suggest targeting broadband investment alongside improvements in local clinical and emergency services, with reimbursement policies that support access to virtual care.

Health-ISAC advises its members to discover patients' telehealth capabilities to review how telehealth and broadband access can further bridge the gap between rural patients and adequate care.

Privacy, Legal & Regulatory

Nothing to Report.

Health-ISAC Cyber Threat Level

On September 17, 2026, the Health-ISAC Threat Intelligence Committee (TIC) evaluated the current Cyber Threat Level and decided to maintain it at **Yellow (Elevated)**. The Threat Level of **Yellow (Elevated)** is due to threats from:

ShinyHunters Activity, Job Scams, Increase in Vulnerability Reporting, Third-Party Risk, and DPRK IT Worker Fraud.

For more information about the Health-ISAC Cyber Threat Level, including definitions and response guidelines for each of the alert levels, please review the Threat Advisory System.

You must have Cyware Access to reach the Threat Advisory System document.

Contact membership@h-isac.org for access to Cyware.

Report Source(s)

Health-ISAC

Reference

[bleepingcomputer](#)

[hipaajournal](#)

[thehackernews](#)

[cyware](#)

[cyware 1](#)

[cyware 2](#)

[bleepingcomputer 1](#)

[healthcareitnews](#)

[securityweek](#)

[thehackernews 1](#)

Tags

TA419, Dell Container Storage Modules, Fortra Core Privileged Access Manager, Fortra BoKS, WarLock, Silver Fox, Fortra, Citrix NetScaler ADC, China-linked cyber espionage group, SAML, Citrix NetScaler Gateway, Citrix, Broadband, SharePoint, Dell

TLP:WHITE: Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

Content Powered by BLACKWIRE Labs:



Access the Health-ISAC Threat Intelligence Portal:

Enhance your personalized information-sharing community with improved threat visibility, alert notifications, and incident sharing in a trusted environment delivered to you via email and mobile apps. Contact membership@h-isac.org for access to Health-ISAC Threat Intelligence Portal (HTIP).

For Questions or Comments:

Please email us at toc@h-isac.org