



Daily Cyber Headlines

[Daily Cyber Headlines](#)☐ TLP:WHITE

Alert ID : c274c1a6

Oct 02, 2026, 04:33 AM



Today's Headlines:

Leading Story

- Fortinet Warns of Critical FortiMail Flaw Exploited in Zero-Day Attacks

Data Breaches & Data Leaks

- Nothing to Report

Cyber Crimes & Incidents

- AI Policy Circles Targeted in China-linked Phishing Operation
- SC WordPress Malware, a Self-Healing Mesh of Loaders, Drop-Ins, and A Blockchain-Controlled Backdoor

Vulnerabilities & Exploits

- Kiteworks Patches Max Severity Code Injection Vulnerability

Trends & Reports

- H1 2026 Healthcare Data Breach Report
- Cloudsmith Finds Gap in Software Supply Chain Defenses

Privacy, Legal & Regulatory

- 16-Year-Old Suspected Leader of KillSec Ransomware Group Arrested

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

Fortinet Warns of Critical FortiMail Flaw Exploited in Zero-Day Attacks

Summary

- Fortinet identified a FortiMail vulnerability allowing unauthorized system access. Administrators should apply updates or disable the IBE feature as a mitigation measure.

Analysis & Action

Fortinet reported a FortiMail vulnerability allowing unauthorized system access. This issue is actively exploited, enabling unauthorized file modifications and command execution on affected devices. For more information, Health-ISAC [published](#) an advisory for this.

Health sector organizations handle sensitive patient data, making email security essential. Exploiting this vulnerability could compromise medical communications, breach patient privacy, and disrupt clinical care services.

Health-ISAC advises its members to immediately apply suggested workarounds, such as disabling the IBE feature, and install official security updates as soon as they become available.

Data Breaches & Data Leaks

Nothing to Report.

Cyber Crimes & Incidents

AI Policy Circles Targeted in China-linked Phishing Operation

Summary

- China-aligned threat actor TA419 targeted U.S. AI policy experts with impersonation-based phishing campaigns designed to steal Microsoft cloud credentials and active sessions, using fake collaboration invitations and adversary-in-the-middle authentication techniques.

Analysis & Action

TA419 conducted targeted credential-phishing campaigns against AI policy experts working at U.S. think tanks, universities, and law firms. The threat actor impersonated prominent economists, former government officials, and an Anthropic employee, initially sending benign messages involving AI policy committees, export controls, supply chains, and military use of AI to establish trust before introducing malicious links.

After a target responded, TA419 delivered shortened URLs that redirected to attacker-controlled infrastructure, which then forwarded to fraudulent OneDrive pages. The campaign used a customized version of the Frameless BitB phishing toolkit and adversary-in-the-middle techniques to relay authentication through legitimate Microsoft infrastructure, allowing passwords, MFA, and conditional access checks to succeed while capturing the resulting session cookies.

Health-ISAC advises its members to reinforce protections against conversation-based phishing and impersonation campaigns, particularly for personnel involved in AI, research, policy, and other sensitive areas. Organizations should deploy phishing-resistant authentication, such as passkeys, where feasible, monitor for suspicious Microsoft 365 session activity, verify unexpected collaboration requests through independent channels, and investigate anomalous cloud logins or session reuse following suspicious communications.

SC WordPress Malware, A Self-Healing Mesh of Loaders, Drop-Ins, and A Blockchain-Controlled Backdoor

Summary

- Researchers identified SC, a persistent WordPress malware family that distributes its backdoor across files, databases, and shared memory, allowing compromised websites to automatically rebuild malicious components even after administrators remove visible infections.

Analysis & Action

Researchers analyzed a WordPress compromise involving malware dubbed SC that maintains at least eight interconnected persistence components. Copies of the payload are distributed across WordPress plugins, drop-ins, theme files, database records, ZIP archives, scheduled tasks, and System V shared memory, allowing surviving components to reconstruct others within seconds after removal.

The backdoor hides itself from WordPress administrators, creates concealed administrator accounts, forges authentication cookies, fingerprints compromised sites, steals active administrator session tokens, and can inject additional PHP or JavaScript payloads. It also uses approximately 20 public Ethereum RPC gateways to retrieve command-and-control instructions from a blockchain smart contract, thereby providing a resilient infrastructure that is more difficult to disrupt via traditional domain blocking.

Health-ISAC advises its members operating WordPress environments to investigate unexpected `auto_prepend_file` directives, unauthorized modifications to `db.php` or `advanced-cache.php`, hidden administrator accounts, suspicious database options, shared-memory payloads, and outbound connections to Ethereum RPC gateways. Organizations should remove all persistence mechanisms in a coordinated cleanup, rotate potentially exposed credentials and sessions, patch WordPress components, and monitor previously affected systems for rapid reinfection.

Vulnerabilities & Exploits

Kiteworks Patches Max Severity Code Injection Vulnerability

Summary

- Kiteworks patched 126 vulnerabilities, including maximum-severity CVE-2026-54154 affecting its Email Protection Gateway. The flaw can allow unauthenticated remote attackers to execute arbitrary code and potentially gain full root control of vulnerable appliances.

Analysis & Action

[CVE-2026-54154](#) affects Kiteworks Email Protection Gateway releases prior to version 9.4.1 and can be exploited remotely without authentication or user interaction.

Successful exploitation exploits multiple weaknesses, including path traversal, code injection, and missing authentication, potentially allowing an attacker to execute arbitrary code on an exposed EPG appliance. For more information, Health-ISAC [published](#) an advisory for this.

Kiteworks also addressed 125 additional vulnerabilities, including 11 critical issues involving authentication bypass, administrator account takeover, stored cross-site scripting, improper access control, and improper authentication across its Core and EPG components. The disclosure follows a separate precautionary shutdown in late September after Kiteworks received intelligence regarding a potentially imminent attack and subsequently remediated another critical vulnerability, for which technical details and a CVE have not yet been released.

Health-ISAC advises its members to identify Kiteworks Email Protection Gateway deployments and upgrade affected systems to version 9.4.1 or later, preferably the latest supported release. Organizations should prioritize internet-facing appliances, restrict administrative interfaces to trusted networks, review systems for suspicious activity or unauthorized configuration changes, and ensure Kiteworks appliances are incorporated into vulnerability management and perimeter monitoring processes.

Trends & Reports

H1 2026 Healthcare Data Breach Report

Summary

- Health sector organizations reported 397 large data breaches in H1 2026, exposing or impermissibly disclosing the protected health information of 33.77 million individuals. Overall breaches declined, while threat actor activity and IT incidents continued to increase.

Analysis & Action

Between January and June 2026, 397 Health sector data breaches affecting 500 or more individuals were reported, representing a 5.9% decline compared with H1 2025 and the lowest first-half total since 2023. Approximately 33.77 million individuals were affected, a 22.6% year-over-year reduction, although large breaches continued to occur at a rate exceeding 2.2 per day.

Threat actor activity and IT incidents remained the leading cause of Health Sector data breaches, accounting for 343 incidents and up 2.1% year over year for the third consecutive year. Nine breaches affected more than one million individuals, while ransomware and data-theft extortion remained significant threats. Network servers continued to be the most common location for breaches of protected health information, with email accounts also remaining a frequent source of exposure.

Health-ISAC advises its members to maintain risk-based cybersecurity programs focused on preventing and detecting hacking, ransomware, data theft, and credential compromise. Organizations should strengthen multifactor authentication, protect internet-facing systems, segment critical infrastructure, maintain tested backups, monitor network servers and email environments for suspicious activity, and conduct regular enterprise risk assessments that include business associates and other third parties handling protected health information.

Cloudsmith Finds Gap in Software Supply Chain Defenses

Summary

- Cloudsmith research identifies a significant gap between confidence in software supply chain defenses and the actual preventive controls in place, with many engineering teams allowing open-source dependencies into environments before performing security checks or responding to malicious packages.

Analysis & Action

Cloudsmith surveyed 400 platform and security engineers in the UK and the US and found that 73% believe their existing tools can stop install-time attacks before security advisories are available. However, only 38% screen dependencies before they enter organizational environments, while just 24% automatically enforce cooldown periods for newly released packages.

The findings indicate that many organizations remain dependent on reactive security measures, with 54% taking action only after malicious code has already entered their systems and another 8% lacking a consistent response. The research also highlights risks associated with relying heavily on provenance and attestation, as legitimate build credentials or pipelines can be compromised while malicious packages retain apparently trustworthy provenance. AI coding agents may further increase exposure by automatically introducing dependencies with limited human review.

Health-ISAC advises its members to strengthen software supply-chain controls by screening third-party and open-source dependencies before they enter development environments. Organizations should consider centralized, pre-approved private repositories, automated cooldown periods for newly published packages, continuous scanning for malicious packages, and policy enforcement at ingestion, while ensuring that AI-assisted development tools follow the same dependency governance and security requirements.

Privacy, Legal & Regulatory

16-Year-Old Suspected Leader of KillSec Ransomware Group Arrested

Summary

- An international operation disrupted the KillSec ransomware group, arresting three suspects and identifying a 16-year-old as its suspected main operator. Authorities seized critical infrastructure and secured at least 110 terabytes of stolen data from victims.

Analysis & Action

KillSec has operated since 2024 as a ransomware and data extortion operation targeting organizations worldwide. Authorities link the group to nearly 1,000 suspected attacks, approximately 500 of which have so far been identified as successful. KillSec commonly gained access by exploiting software vulnerabilities and poorly secured entry points, particularly cloud storage, before stealing sensitive information and threatening to publish it unless victims paid.

Operation KillSwitch resulted in three provisional arrests, eight property searches, seizure of five central servers, and law enforcement control of KillSec's leak site and domains. Investigators identified a 16-year-old as the suspected administrator and main operator, along with individuals suspected of acting as a developer, negotiator, and affiliate. Authorities also found that KillSec used AI to help build and maintain ransomware infrastructure and identify potential victims.

Health-ISAC advises its members to reduce exposure to ransomware and data-extortion operations by securing internet-facing systems and cloud storage, rapidly remediating exploitable vulnerabilities, and enforcing strong authentication and least-privilege access. Organizations should monitor cloud repositories for unauthorized access or bulk downloads, maintain tested incident response procedures, and continue monitoring for KillSec-related data exposure as authorities analyze seized infrastructure and victim information.

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

[securitybrief](#)
[helpnetsecurity](#)
[cyberscoop](#)
[bleepingcomputer](#)
[hipaajournal](#)
[cyware](#)
[cyware 1](#)
[sucuri](#)
[bleepingcomputer 1](#)

Tags

CVE-2026-54154, SC WordPress Malware, KillSec Ransomware, CVE-2026-104286, Kiteworks, Fortinet FortiMail, Supply Chain, Fortinet

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