



Daily Cyber Headlines

Daily Cyber Headlines

☐ TLP:WHITE

Alert ID : 6d41d4c4

Oct 07, 2026, 04:56 AM



Today's Headlines:

Leading Story

- Atlassian Warns of Critical File-Access Flaw in Jira, Confluence

Data Breaches & Data Leaks

- Ransomware Attack Disrupts Medical School Systems and Exfiltrates Data

Cyber Crimes & Incidents

- Fake ChatGPT, Gemini Sites Steal Advertising Accounts, MFA Codes
- Belarusian Threat Actors Spent Two Years Inside a Healthcare Network

Vulnerabilities & Exploits

- LibreOffice and OpenOffice Flaws Let Malicious Spreadsheets Run Code Without Macro Warnings

Trends & Reports

- FortiBleed Remains Active Campaign, Can Lock Out Users or Lead to Ransomware Attacks

Privacy, Legal & Regulatory

- [OpenAI Adds Invisible Watermarks to Generated Text to Meet AI Transparency Rules](#)

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

[Atlassian Warns of Critical File-Access Flaw in Jira, Confluence](#)

Summary

- Atlassian issued a security advisory warning of a critical arbitrary file-access vulnerability (CVE-2026-21589) across self-hosted Data Center products, including Confluence, Jira, and Bitbucket. Unauthenticated remote attackers can access sensitive system files residing in the web root directory.

Analysis & Action

Atlassian published security updates addressing a critical arbitrary file-access vulnerability, tracked as CVE-2026-21589, that affects multiple self-hosted Atlassian Data Center and Server products. Impacted solutions include Confluence Data Center, Jira Software Data Center, Jira Service Management Data Center, Bitbucket Data Center, Bamboo Data Center, Crowd Data Center, Crucible, and Fisheye. Atlassian confirmed that its cloud-hosted SaaS offerings are not affected, and no active in-the-wild exploitation has been publicly reported to date. For more information, Health-ISAC [published](#) an advisory for this.

The vulnerability enables unauthenticated remote attackers to request and read specific files stored within the web application root directory of affected instances. Exploitation requires the attacker to know the target file's exact name and path, as the flaw does not allow directory listing or path enumeration.

Health-ISAC advises its members to immediately upgrade all self-hosted Atlassian Data Center installations to patched versions, including Confluence Data Center 9.2.26 / 10.2.19, Jira Software 9.12.40 / 10.3.26 / 11.3.12, Bitbucket Data Center 9.4.26 / 10.2.8 / 10.5.1, and corresponding fixes for Bamboo, Crowd, Crucible, and Fisheye. Security teams should restrict public web access to administrative and self-hosted collaboration

portals and enforce network segmentation and VPN controls. Additionally, organizations should audit web server logs for suspicious or abnormal direct HTTP GET requests targeting specific web root files from unauthenticated IP addresses.

Data Breaches & Data Leaks

Ransomware Attack Disrupts Medical School Systems and Exfiltrates Data

Summary

- The University of Illinois Chicago (UIC) in Chicago, Illinois, confirmed a ransomware attack that temporarily disrupted College of Medicine systems and resulted in data theft. The university reports that its main network and patient care at UI Health were not affected.

Analysis & Action

The Booba Project ransomware operation listed UIC on its leak site on October 2, 2026, claiming to have exfiltrated 344 gigabytes (GB) of data, a figure that remains unverified. UIC is investigating whether personal, research, or academic information was compromised, and affected systems have been restored.

Booba Project emerged in late July 2026 and is assessed as a rebrand of the Frag ransomware, deploying Windows and Linux encryptors that append the .booba extension. The initial access vector has not been disclosed.

Health-ISAC advises its members to segment academic and research environments from clinical networks, enforce Multi-Factor Authentication (MFA) on all remote access, and maintain offline, tested backups for Windows and Linux systems. Organizations should monitor for large outbound data transfers and files with the .booba extension on servers hosting research or student data

Cyber Crimes & Incidents

Fake ChatGPT, Gemini Sites Steal Advertising Accounts, MFA Codes

Summary

- Threat actors deployed counterfeit versions of ChatGPT, Gemini, Claude, and Perplexity to target digital marketing and advertising account managers. The social engineering campaign uses Browser-in-the-Browser phishing kits to steal

login credentials, intercept multi-factor authentication codes, and hijack connected corporate advertising accounts.

Analysis & Action

Threat actors deployed deceptive landing pages that mimicked popular generative AI platforms, including ChatGPT, Gemini, Claude, Perplexity, and Manus, promising specialized advertising management, automated campaign planning, and Google Ads integration. The adversary's underlying objective is not to compromise the AI platforms themselves, but to harvest credentials to hijack high-value connected corporate advertising accounts on platforms such as Google Ads, Meta Business Manager, and Okta.

Built on Next.js and Socket.IO, hosted across Vercel, Railway, and Render, and orchestrated via Telegram, this phishing platform replaces traditional reverse proxies with locally rebuilt login interfaces and Browser-in-the-Browser (BitB) fake OAuth windows. Human operators monitor victim interactions in real time over WebSockets, dynamically requesting passwords and multi-factor authentication (MFA) prompts to capture valid session tokens.

Health-ISAC advises its members to deploy phishing-resistant authentication methods, such as FIDO2 passkeys or hardware security keys, which cannot be intercepted by Browser-in-the-Browser proxy workflows. Organizations should educate marketing, communications, and administrative personnel to recognize BitB artifacts, such as pop-up windows that cannot be dragged outside the main browser viewport or resized.

Belarusian Threat Actors Spent Two Years Inside a Healthcare Network

Summary

- Russian cybersecurity firm Solar discovered an intrusion by a Belarusian threat group into the network of a Russian healthcare organization, potentially allowing access to sensitive medical data.

Analysis & Action

The Belarusian Cyber Partisans emerged following mass protests against Belarusian President Alexander Lukashenko after the country's disputed 2020 presidential election. They have since claimed responsibility for some of the largest cyberattacks against the Belarusian government, including operations targeting state institutions and the country's railway system.

The Russian cybersecurity firm Solar states that the target organization operated extensive infrastructure with connections to numerous other healthcare organizations, potentially giving threat actors opportunities to use the compromised network to reach additional attack surfaces.

Health-ISAC advises its members to continue using safe cybersecurity measures, given that certain threat actors target the healthcare sector in hopes of gaining information that could assist in attacking other sectors and government systems.

Vulnerabilities & Exploits

LibreOffice and OpenOffice Flaws Let Malicious Spreadsheets Run Code Without Macro Warnings

Summary

- A newly disclosed vulnerability affecting LibreOffice and Apache OpenOffice enables malicious spreadsheets to execute arbitrary code automatically upon opening, bypassing security warnings normally triggered by macros.

Analysis & Action

This security flaw leverages standard spreadsheet capabilities to achieve exploitation. By utilizing database range parameters, a spreadsheet references an external database file (ODB) hosted at a web link. Upon launch, the software fetches the ODB file, which references a distant Java database driver. The system then retrieves and executes this driver code locally, bypassing any user authorization or trust prompts.

To succeed, the vector requires enabling Java functionality within the productivity software, affecting both Windows and Linux platforms. Analysts have successfully created a functional proof of concept that launches local software, though adversaries could leverage it to execute arbitrary code payloads.

Health-ISAC advises its members to deploy official vendor updates promptly. Additionally, OpenOffice users can reduce their exposure by disabling Java integration in the software's options or by refraining from opening unverified files.

Trends & Reports

FortiBleed Remains Active Campaign, Can Lock Out Users or Lead to Ransomware Attacks

Summary

- The Federal Bureau of Investigation (FBI) and United States Secret Service (USSS) released a joint advisory on October 6, 2026, warning that the FortiBleed campaign continues to target internet-facing Fortinet FortiGate firewalls. The advisory applies to all United States critical infrastructure sectors, including Healthcare and Public Health.

Analysis & Action

FortiBleed abuses reused or leaked credentials and legacy password storage rather than a software vulnerability, with compromised devices now exceeding 86,644 across 194 countries. Operators crack harvested credentials offline and sell access to ransomware affiliates, including INC/Lynx and Payload.

After intrusion, the actors create rogue administrator accounts such as fortiAdmin and support_fortinet, and in some cases delete legitimate accounts, locking administrators out of their own devices.

Health-ISAC recommends disabling public internet access to firewall management interfaces, enforcing multifactor authentication, resetting administrative credentials, and monitoring access logs for unauthorized changes and lateral movement. Health-ISAC also recommends checking the [published](#) advisory as well regarding FortiBleed in June 2026.

Privacy, Legal & Regulatory

OpenAI Adds Invisible Watermarks to Generated Text to Meet AI Transparency Rules

Summary

- OpenAI announced on October 5, 2026, that it will embed an invisible watermark in eligible ChatGPT and Codex text generated in the European Union (EU). The rollout, expected over the coming weeks, addresses transparency requirements under the EU Artificial Intelligence (AI) Act.

Analysis & Action

The system, called textGrain, adds a hidden statistical signal to the model's word choices rather than inserting hidden characters. Article 50 of the AI Act requires

providers of generative AI systems to mark text outputs in a machine-readable way, with existing providers required to comply by December 2, 2026. Anthropic, Google, Meta, and Microsoft have also committed to the EU Code of Practice on AI-generated content.

[OpenAI acknowledges](#) significant limitations. Detection succeeded in roughly 80% of 200-token test passages, editing weakens the signal, and the detector can produce false positives.

Health-ISAC advises its members to review generative AI governance and acceptable use policies for EU operations, and to inventory where AI-generated text enters clinical, research, and patient communication workflows. Organizations should avoid treating the presence or absence of a watermark as proof of authorship in fraud or misconduct investigations.

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

[ic3](#)
[bleepingcomputer](#)
[thehackernews](#)
[bleepingcomputer 1](#)

cyware
therecord
cyware 1
openai
atlassian
therecord 1
cyberscoop

Tags

AI Transparency Rules, Medical School, CVE-2026-21589, FortiBleed, Gemini AI, OpenAI, ChatGPT, OpenOffice, Belarus, LibreOffice., Atlassian, Macro

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