

Daily Cyber Headlines

Daily Cyber Headlines

TLP:WHITE

Alert ID : 055a178d

Oct 01, 2025, 06:02 AM



Today's Headlines:

Leading Story

- VMware Tools and Aria Zero-Day Vulnerability Exploited to Escalate Privileges and Execute Code as Root

Data Breaches & Data Leaks

- Threat Actor Claims Global AT&T, Mercedes Partner
- Threat Actors Exfiltrate FEMA, Customs and Border Protection Staff Data

Cyber Crimes & Incidents

- Lunar Spider Infected Windows Machine in Single Click to Harvest Login Credentials

Vulnerabilities & Exploits

- Threat Actors Actively Scanning to Exploit Palo Alto Networks PAN-OS Global Protect Vulnerability

Trends & Reports

- EvilAI Malware Masquerades as AI Tools to Infiltrate Global Organizations
- Acreed Infostealer Used Widely by Cybercriminals With C2 Via Steam Platform

Privacy, Legal & Regulatory

- [California Gov. Gavin Newsom Signs Bill Creating AI Safety Measures](#)

Upcoming Health-ISAC Events

- Global Monthly Threat Brief
 - European – October 1, 2025, 03:00-04:00 PM CET
- [European Summit](#) – Rome, Italy – October 14-16, 2025
- [Fall Americas Summit](#) – Carlsbad, California – December 1-5, 2025

Additional Information

Leading Story

[VMware Tools and Aria Zero-Day Vulnerability Exploited to Escalate Privileges and Execute Code as Root](#)

Summary

- NVISO researchers discovered that threat actors are actively exploiting a zero-day vulnerability in VMware Tools and VMware Aria Operations that grants root-level privileges for a complete system takeover.

Analysis & Action

A new zero-day vulnerability in VMware Tools and VMware Aria Operations is actively being exploited, enabling threat actors to gain root-level code execution capabilities.

The flaw, CVE-2025-41244, lies in an untrusted search path in a system script that identifies service versions running on virtual environments. Threat actors are exploiting the weakness by embedding malicious executables, often named as system binaries, in path directories that, when run, grant them elevated privileges to gain complete control over the system. NVISO researchers have attributed the current exploits to the Chinese threat group UNC5174.

Health-ISAC recommends that its members actively monitor for suspicious system activity, regularly apply software patches, and scan for any potential vulnerabilities as mitigation measures.

Data Breaches & Data Leaks

[Threat Actor Claims Global AT&T, Mercedes Partner](#)

Summary

- A threat actor has claimed to have breached the global boutique consulting firm Credera and stolen information on its major partners.

Analysis & Action

The threat actor claims to have breached Credera, a global boutique consulting firm, stating they have stolen information about their major clients.

The clients affected by the breach were AT&T, Mercedes, Green Dot, Myze, and Spectrio. Data, which is available for purchase at the time of reports, supposedly includes Credera confidential documents, Terraform files, Internal customer documents, source code, SSL certificates, SMTP credentials, API keys, private and public keys, SQL files, GitHub projects, Pipeline builds, and internal projects. The threat actor has released screenshots as evidence of the breach. Researchers warn that the exposed source code, software architecture, and SQL files could result in further vulnerability exploitation.

Health-ISAC advises its members to consider network segmentation, encryption of all sensitive data, and offline backups of sensitive data as mitigations to data breaches and leaks.

[Threat Actors Exfiltrate FEMA, Customs and Border Protection Staff Data](#)

Summary

- Threat actors targeting the Federal Emergency Management Agency (FEMA) exfiltrated sensitive data belonging to employees of both FEMA and US Customs and Border Protection (CBP).

Analysis & Action

Threat actors have breached government systems and exfiltrated employee data from the United States Federal Emergency Management Agency (FEMA) and the US Customs and Border Protection (CBP).

The breach allegedly began on June 22, when an unauthorized user leveraged compromised credentials to access FEMA's Region 6 Citrix Systems software. The threat actor remained undetected for weeks, exfiltrating sensitive employee data from the agency and the CBP. The Department of Homeland Security (DHS) attributed the incident to weak cybersecurity frameworks that failed to protect government systems, including a lack of user authentication protocols and inefficient patching schedules.

Health-ISAC encourages its members to employ multi-factor authentication for all accounts, frequently scan for and patch system vulnerabilities, and actively monitor network activity to mitigate data breaches.

Cyber Crimes & Incidents

[Lunar Spider Infected Windows Machine in Single Click to Harvest Login Credentials](#)

Summary

- A newly identified malware strain, Lunar Spider, threatens Windows environments, compromising systems with one click.

Analysis & Action

A newly discovered malware strain, Lunar Spider, has emerged, posing possible threats to Windows environments by compromising systems with a single click.

The strain was initially detected in mid-September 2025, when victims saw a seemingly harmless link through phishing emails or instant messaging platforms. Once the victim clicks this, Lunar Spider begins a stealthy download of its key components, utilizing legitimate Windows utilities to avoid detection. The malware then scans for active user sessions. It begins harvesting stored credentials, sometimes used to laterally move throughout networks to further exfiltrate sensitive documents and financial records without user awareness of compromise.

Health-ISAC advises its members to consider leveraging reputable antivirus software alongside enabling firewalls as mitigations against similar attack vectors.

Vulnerabilities & Exploits

[Threat Actors Actively Scanning to Exploit Palo Alto Networks PAN-OS Global Protect Vulnerability](#)

Summary

- A critical PAN-OS GlobalProtect vulnerability permits threat actors to execute complete root code execution on vulnerable firewalls.

Analysis & Action

Cybersecurity researchers have observed a concerning rise in scans targeting a PAN-OS GlobalProtect vulnerability, tracked as CVE-2024-3400 (CVSS v3.1 score of 10.0)

Observed exploitation attempts of the flaw show threat actors looking to utilize the arbitrary file creation flaw to commit OS command injection, resulting in complete root code execution on vulnerable firewalls. The vulnerability affects PAN-OS 10.2 versions before 10.2.9-h1, 11.0 versions before 11.0.4-h1, and 11.1 versions before 11.1.2-h3. Palo Alto Networks has since released fixed PAN-OS versions of 10.2.9-h1, 11.0.4-h1, and 11.1.2-h3, advising its users to upgrade to prevent exploitation immediately.

Health-ISAC advises its members to verify firewall configurations and regularly revisit logs to detect and mitigate similar vulnerability exposure.

Trends & Reports

[EvilAI Malware Masquerades as AI Tools to Infiltrate Global Organizations](#)

Summary

- Trend Micro has disclosed a new campaign, EvilAI, that disguises malicious versions of legitimate software to target critical infrastructure worldwide.

Analysis & Action

Trend Micro has identified a new campaign, tracked as EvilAI, targeting major global companies by leveraging legitimate AI-powered software to deploy malware.

The operation has targeted critical infrastructure from central European, Asian-Pacific, and American organizations, including healthcare. Threat actors disguise the campaign's malicious activity through deceptive versions of legitimate software—such as PDF Editor and AppSuite—that contain valid digital signatures to bypass established security protocols. As per the reports, EvilAI is used to gain initial access and establish persistence for additional payloads.

Health-ISAC encourages its members to deploy endpoint detection tools, actively monitor network activity, and limit software downloads from unofficial sources to mitigate similar threats.

[Acreed Infostealer Used Widely by Cybercriminals With C2 Via Steam Platform](#)

Summary

- Cybersecurity specialists have been tracking the emerging Acreed infostealer, which can steal web browser data with minimal detection.

Analysis & Action

Cybersecurity specialists have been tracking threat activity primarily from Russian-speaking cybercriminal forums that leverage the emerging Acreed information stealer.

The infostealer was first detected in February of this year and stood out from other malware due to its minimalist logging. The infection chain begins with the deployment of ShadowLoader via trojanized payloads, which, once installed, use a dead-drop resolver to retrieve the target C2 domain. Acreed exfiltrates passwords and cookies and stores autofill data from Chrome, Edge, and Brave browsers.

Health-ISAC advises its members to avoid installing software from untrusted sources, deploying endpoint detection tools, and actively monitoring network traffic as mitigation measures.

Privacy, Legal & Regulatory

[California Gov. Gavin Newsom Signs Bill Creating AI Safety Measures](#)

Summary

- California's governor has signed a law to prevent the use of powerful AI models for catastrophic activities.

Analysis & Action

California's governor, Gavin Newsom, has signed a law establishing first-in-the-nation regulations on large-scale AI models. The law intends to prevent individuals from using AI models for catastrophic activities.

The law, dubbed the Transparency in Frontier Artificial Intelligence Act (TFAIA), will aim to stop individuals from using powerful artificial intelligence models for activities that could be harmful, such as building bioweapons or shutting down vital systems like banks. The new law will require California-based AI companies to both implement and disclose public safety protocols in hopes of mitigating the risks of their being used for malicious purposes. The development comes as high-performing generative AI systems are expected to become more powerful, with existing systems made mainly in companies based in California, such as Anthropic, Google, Meta, and OpenAI.

Health-ISAC advises its members to consider implementing a zero-trust framework and vet open source models to mitigate possible generative AI attacks.

Health-ISAC Cyber Threat Level

On September 18, 2025, the Health-ISAC Threat Intelligence Committee (TIC) evaluated the current Cyber Threat Level and collectively decided to maintain the Cyber Threat Level to **Blue (Guarded)**. The Threat Level of **Blue (Guarded)** is due to threats from:

NPM Worm Impact, QR Code Phishing, Typosquatting Campaigns, Remote IT Worker Fraud, and Job Posting Scams.

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

Tags

AI Safety, Acreed Infostealer, EvilAI, Lunar Spider, Palo Alto, Data Breaches, VMware

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

Share Threat Intel:

For guidance on sharing indicators with Health-ISAC via HTIP, please visit the Knowledge Base article "HTIP - Share Threat Intel" [here](#).

The "Share Threat Intel" feature allows for attributed or anonymous sharing across ISACs and other cybersecurity-related entities.

Turn off Categories:

For guidance on disabling alert categories, please visit the Knowledge Base article "HTIP Alert Categories" [here](#).

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