Daily Cyber Headlines

Oct 30, 2026

WHITE

View Alert

Today's Headlines:

Leading Story

- Cisco Patches Actively Exploited ASA and FTD VPN Flaw That Can Crash Firewalls

Data Breaches & Data Leaks

- 26,400 Valid Cloud and AI Credentials Found Exposed in Public Gitee Repositories

Cyber Crimes & Incidents

- Fake Health Camps Used to Facilitate E-SIM Cyber Fraud Through Identity Theft

Vulnerabilities & Exploits

- Telegram Android Flaw Lets Threat Actors Run Code When Users Answer Voice Calls
- Warp Panda Exploits VMware ESX Zero-Day to Evade Audit Logging

Trends & Reports

- Google Introduces Gemini 4 Carbon With Advanced Cybersecurity Capabilities
- Threat Actors Could Poison AI Models by Tampering With Core Infrastructure

Privacy, Legal & Regulatory

- Nothing To Report

Upcoming Health-ISAC Events

- Global Monthly Threat Brief
    - Americas – November 24, 2026, 12:00 PM - 1:00 PM ET
    - European – November 25, 2026, 03:00-04:00 PM CET
    - APAC – November 27, 2026, 01:00-02:00 PM AEST

Additional Info

Leading Story

Cisco Patches Actively Exploited ASA and FTD VPN Flaw That Can Crash Firewalls

Summary

- Cisco patched an actively exploited vulnerability affecting Adaptive Security Appliance (ASA) and Secure Firewall Threat Defense (FTD) products. Unauthenticated VPN requests can trigger unexpected firewall restarts, potentially disrupting critical network services.

Analysis & Action

These firewall platforms provide network protection and remote-access services for enterprise environments. In hospitals, repeated device restarts could interrupt staff VPN sessions, connections to external systems, and the availability of dependent clinical services.

CVE-2026-76418 (CVSS 8.6) affects VPN tunnel groups using secondary authentication, allowing crafted requests to restart vulnerable firewalls without successful login. Cisco confirms active exploitation but has not identified the responsible threat actors.

Health-ISAC advises its members to inventory ASA and FTD devices, verify secondary-authentication tunnel configurations, deploy fixed releases, investigate unexpected firewall restarts, and coordinate updates with clinical teams to maintain service continuity.

Data Breaches & Data Leaks

26,400 Valid Cloud and AI Credentials Found Exposed in Public Gitee Repositories

Summary

- An independent researcher identified 26,400 valid cloud and artificial intelligence credentials across 7.25 million public Gitee code repositories, exposing organizations to potential unauthorized service access, resource misuse, and sensitive data compromise.

Analysis & Action

An investigation of Gitee, a public source-code hosting platform, uncovered widespread credential exposure across development repositories and their historical commits. The findings demonstrate how inadvertently published secrets can remain usable long after code changes.

Researchers verified application programming interface (API) keys using two scanners, including 9,473 Alibaba Cloud credential pairs and thousands of AI service keys. Historical commits retained some exposed secrets, while misuse and revocation remain unconfirmed.

Health-ISAC advises its members to scan public repositories and commit histories for exposed secrets, immediately revoke and rotate compromised keys, apply least-privilege access, review associated usage logs, and prevent future credential commits.

Cyber Crimes & Incidents

Fake Health Camps Used to Facilitate E-SIM Cyber Fraud Through Identity Theft

Summary

- In New Delhi, India, Police arrested two suspects accused of using fake health camps to harvest identity and biometric information for fraudulent SIM

activations. Investigators linked the resulting phone numbers to cyberfraud complaints involving substantial financial losses.

Analysis & Action

Investigators say the suspects posed as health camp organizers offering discounted medicines in rural areas, then misused participants' identity details to obtain mobile connections. The scheme exploited trust in health-related services, rather than compromising a confirmed healthcare provider.

Police reported more than 3,000 activated SIM cards, including e-SIMs (embedded subscriber identity modules), distributed through a resale network. Some numbers were used in digital arrest scams, involving impersonation of authorities and financial coercion.

Health-ISAC advises its members to verify the legitimacy of community health events, prevent unauthorized collection of patient identifiers or biometrics, educate staff about impersonation scams, and establish reporting channels for suspicious health-related outreach.

Vulnerabilities & Exploits

Telegram Android Flaw Lets Threat Actors Run Code When Users Answer Voice Calls

Summary

- Researchers disclosed a Telegram for Android call-handling flaw that, when chained with additional vulnerabilities, could enable code execution after a user answers a voice call. The issue is fixed in version 12.10.4.

Analysis & Action

Security researchers demonstrated an attack against Telegram's Android application involving incoming voice calls. The reported exploit chain requires the recipient to answer and additional vulnerabilities to escape the application and potentially compromise the device.

Improper handling of MediaState call-signaling messages could access an absent field in memory. Researchers claim chaining this issue with an information leak and separate Android root exploit enabled full device control; independent technical details remain limited.

Health-ISAC advises its members to update Telegram for Android to version 12.10.4 or later, verify application versions on managed devices, restrict calls from unknown users, and investigate suspicious mobile activity following unexpected calls.

Warp Panda Exploits VMware ESX Zero-Day to Evade Audit Logging

Summary

- Researchers linked Warp Panda to exploitation of a VMware ESX logging vulnerability during espionage intrusions. The flaw allows administrators to perform certain actions without audit records, weakening investigations despite its low severity rating.

Analysis & Action

Newly published threat intelligence identifies Warp Panda exploiting a previously disclosed VMware ESX weakness during intrusions affecting legal-sector organizations. The activity illustrates how compromised virtualization administrators can conceal actions and prolong unauthorized access.

CVE-2026-41709 is an insufficient logging flaw requiring administrator privileges; it does not provide initial access. Investigators observed exploitation alongside VMware vCenter malware deployment and other techniques for maintaining covert access.

Health-ISAC advises its members to patch affected VMware ESX hosts, review privileged administrative accounts, forward virtualization logs to independent monitoring systems, investigate suspicious vCenter activity, and validate audit coverage across critical clinical infrastructure.

Trends & Reports

Google Introduces Gemini 4 Carbon With Advanced Cybersecurity Capabilities

Summary

- Google announced Gemini 4 Carbon, reporting improved performance in detecting software vulnerabilities, validating their exploitability, and generating patches, with a phased release to approved security organizations.

Analysis & Action

The model's reported capabilities show how advanced AI could support vulnerability assessments, exploitability analysis, and software remediation. Such developments may help security teams address complex weaknesses, although independent testing remains necessary to establish operational reliability.

Gemini 4 Carbon achieved 88.2% on SEC-bench Pro for vulnerability discovery, 54.8% on ExploitGym for exploitation, and 71.0% on CWE-bench for patching. These evaluations were conducted under benchmark conditions without cybersecurity guardrails.

Health-ISAC advises its members to establish governance for AI-assisted security testing, verify vulnerability findings, and assess generated patches for unintended consequences. Security teams should restrict sensitive data exposure and maintain established vulnerability prioritization procedures.

Threat Actors Could Poison AI Models by Tampering With Core Infrastructure

Summary

- Researchers showed that compromised AI infrastructure can alter a model's behavior by changing in-memory parameters while the original files and digital signatures remain intact. The findings highlight security risks beyond conventional model-integrity checks.

Analysis & Action

New technical research shows how weaknesses in the underlying hardware and firmware that support artificial intelligence can undermine model integrity. The findings raise concerns for organizations deploying AI in clinical, development, and security workflows.

Researchers used a data processing unit (DPU), a specialized infrastructure processor, and permissive memory-access configurations to modify live model parameters. Stored files passed integrity checks, although the technique was demonstrated under controlled laboratory conditions.

Health-ISAC advises its members to inventory AI infrastructure components, secure hardware management interfaces, enforce memory-access isolation, verify firmware integrity, and assess runtime monitoring capabilities before relying on AI systems in sensitive clinical or security workflows.

Privacy, Legal & Regulatory

Nothing to report.

Health-ISAC Cyber Threat Level

On October 15, 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:

IT Worker Fraud, Holiday Scams, Job Scams, Sustained Increase in Vulnerability Reporting, The Com Activity.

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.

<hr size=1 width="100%" align=center>

Alert Id	1e6ac194
Category	Daily Cyber Headlines
References	cyware smallbiztrends indiatimes thehackernews thehackernews thehackernews cyware cybersecuritydive thehackernews
Tags	E-SIM, Gitee, Cloud and AI, Gemini AI, WARP, Telegram, Cisco, Google

---

Report Source(s)

Health-ISAC

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

Please provide your feedback

Like Dislike

Download the App
Available on iOS, Android and Web





For more updates and alerts, visit: **https://health-isac.cyware.com/webapp/**
Health-ISAC is an invite only platform. Please DO NOT forward this email to anyone. If you are not supposed to receive this email, please report to **toc@h-isac.org**

--
You received this message because you are subscribed to the Google Groups "TLP Green - Health-ISAC Partners" group.
To unsubscribe from this group and stop receiving emails from it, send an email to health-isac-partners+unsubscribe@h-isac.org.
To view this discussion visit https://groups.google.com/a/h-isac.org/d/msgid/health-isac-partners/010001a18bfa6058-97c373f1-b354-4c20-9867-f95dccdb0656-000000%40email.amazonses.com.