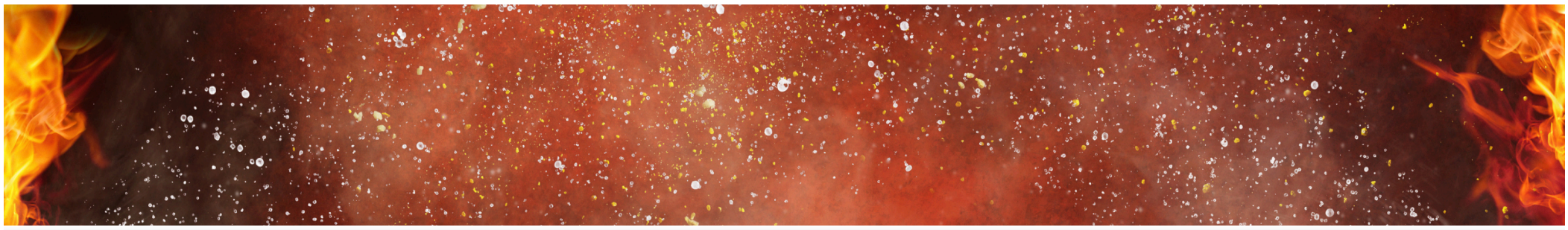


Week of August 4, 2025

Cybersecurity Headlines

Digital Threat Landscape

Cybercrimes, Scams, Threats, Vulnerabilities and Incidents

New 'Plague' PAM Backdoor Exposes Critical Linux Systems to Silent Credential Theft - The Hacker News

thehackernews.com

Cybersecurity researchers have flagged a previously undocumented Linux backdoor dubbed Plague that has managed to evade detection for a year. "The implant is built as a malicious PAM (Pluggable Authentication Module), enabling attackers to silently b...

Gen Z in the Crosshairs: Cybercriminals Shift Focus to Young, Digital-Savvy Workers

www.securityweek.com

Many of the attacks are the same as everyone faces – it's just that Gen Z presents more opportunities to the attacker. Kaspersky focuses on one area – fake employment opportunities that play on the polyworking lifestyle. Perhaps assisted by AI, modern job openings can appear very legitimate, and may be coupled with fake job interviews. But Gen Z, quite simply, is especially susceptible to social e

Who Got Arrested in the Raid on the XSS Crime Forum?

krebsonsecurity.com

On July 22, 2025, the European police agency Europol said a long-running investigation led by the French Police resulted in the arrest of a 38-year-old administrator of XSS, a Russian-language ...

Industry Updates

Legislation, Business, Privacy, Updates, Related Technologies

CISA issues emergency directive requiring federal agencies to update systems to prevent Microsoft Exchange vulnerability | CISA

www.cisa.gov

WASHINGTON – Today, the Cybersecurity and Infrastructure Security Agency (CISA) issued Emergency Directive 25-02 in response to a vulnerability that impacts hybrid Microsoft Exchange users. This post-authentication vulnerability allows a cyber threat...

CISA Adds 3 D-Link Vulnerabilities to KEV Catalog Amid Active Exploitation Evidence - The Hacker News

thehackernews.com

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) on Tuesday added three old security flaws impacting D-Link Wi-Fi cameras and video recorders to its Known Exploited Vulnerabilities (KEV) catalog, based on evidence of active exploitati...

Microsoft Launches Project Ire to Autonomously Classify Malware Using AI Tools - The Hacker News

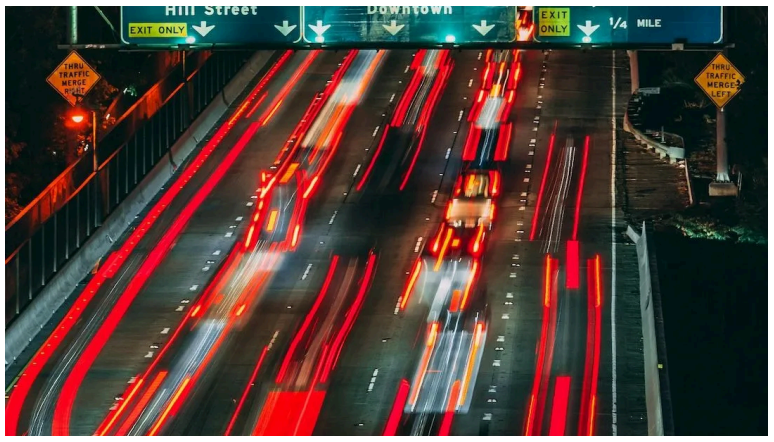
thehackernews.com

Microsoft on Tuesday announced an autonomous artificial intelligence (AI) agent that can analyze and classify software without assistance in an effort to advance malware detection efforts. The large language model (LLM)-powered autonomous malware cla...

Google's August Patch Fixes Two Qualcomm Vulnerabilities Exploited in the Wild

thehackernews.com

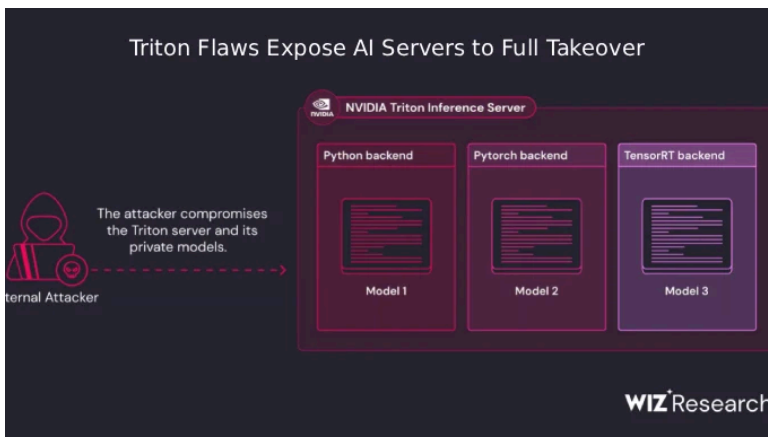
Google has released security updates to address multiple security flaws in Android, including fixes for two Qualcomm bugs that were flagged as actively exploited in the wild.



Strong regulation can nudge automakers to improve customers' privacy, research suggests

therecord.media

New research asserts that while few automakers strongly protect website and customer portal users' privacy, one company drastically improved its practices after California's privacy regulator fined it in March for allegedly failing to implement relevant standards required under state law.



NVIDIA Triton Bugs Let Unauthenticated Attackers Execute Code and Hijack AI Servers - The Hacker News

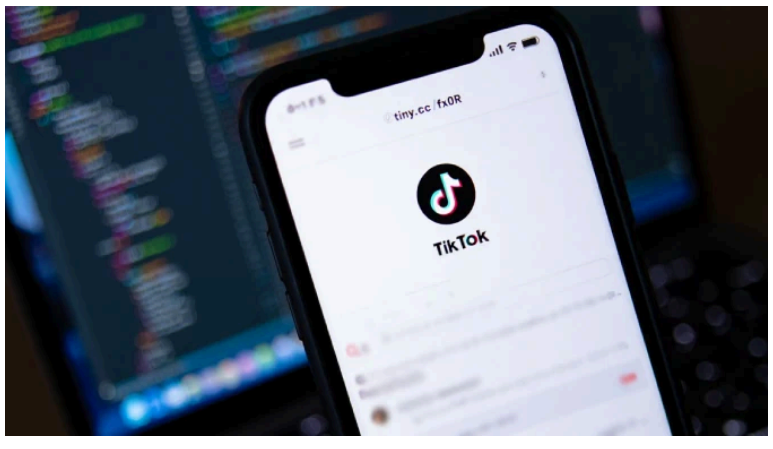
thehackernews.com

A newly disclosed set of security flaws in NVIDIA's Triton Inference Server for Windows and Linux, an open-source platform for running artificial intelligence (AI) models at scale, could be exploited to take over susceptible servers. "When chained to...

CISA pledges to continue backing CVE Program after April funding fiasco

therecord.media

Federal officials told an audience at the Black Hat conference that the Trump administration fully supports and wants to improve the CVE Program, which is heavily used to track and share cybersecurity vulnerabilities.



15,000 Fake TikTok Shop Domains Deliver Malware, Steal Crypto via AI-Driven Scam Campaign - The Hacker News

thehackernews.com

What's more, a chunk of these phishing pages lure users into depositing cryptocurrency on fraudulent storefronts by advertising fake product listings and heavy discounts. CTM360 said it identified no less than 5,000 URLs that are set up with an inten...

Federal judiciary tightens digital security as it deals with 'escalated cyberattacks'

therecord.media

The statement followed a Wednesday report from Politico revealing a major hack of the courts' case filing system which officials feared exposed the identities of confidential informants in criminal cases.

External Quick links

- AIScoop
- BleepingComputer
- Cisco Talos Intelligence Group
- CSO Online
- CyberScoop
- Cybersecurity Dive
- Cyware
- CyberWire
- FedScoop
- Government Executive
- Government Technology
- ISACA
- ISSA International
- Krebs on Security
- MITRE ATT&CK®
- NASCIO
- Schneier on Security
- SC Media
- StateScoop
- The Hacker News
- The Record