Scottish
Cyber
Coordination
Centre

Daily Threat Bulletin

26 August 2025

Vulnerabilities

Critical Docker Desktop flaw lets attackers hijack Windows hosts

BleepingComputer - 25 August 2025 12:11

A critical vulnerability in Docker Desktop for Windows and macOS allows compromising the host by running a malicious container, even if the Enhanced Container Isolation (ECI) protection is active. [...]

⚡ Weekly Recap: Password Manager Flaws, Apple 0-Day, Hidden AI Prompts, In-the-Wild Exploits & More

The Hacker News - 25 August 2025 18:47

Cybersecurity today moves at the pace of global politics. A single breach can ripple across supply chains, turn a software flaw into leverage, or shift who holds the upper hand. For leaders, this means defense isn't just a matter of firewalls and patches—it's about strategy. The strongest organizations aren't the ones with the most tools, but the ones that see how cyber risks connect to business.

CISA Adds Three Known Exploited Vulnerabilities to Catalog

CISA Advisories -

CISA has added three new vulnerabilities to its Known Exploited Vulnerabilities (KEV) Catalog, based on evidence of active exploitation: CVE-2024-8069 Citrix Session Recording Deserialization of Untrusted Data Vulnerability, CVE-2024-8068 Citrix Session Recording Improper Privilege Management Vulnerability, CVE-2025-48384 Git Link Following Vulnerability.

Threat actors and malware

Surge in coordinated scans targets Microsoft RDP auth servers

BleepingComputer - 25 August 2025 20:43

Internet intelligence firm GreyNoise reports that it has recorded a significant spike in scanning activity consisting of nearly 1,971 IP addresses probing Microsoft Remote Desktop Web Access and RDP Web Client authentication portals in unison, suggesting a coordinated reconnaissance campaign. [...]

New AI attack hides data-theft prompts in downscaled images

BleepingComputer - 25 August 2025 18:34

Researchers have developed a novel attack that steals user data by injecting malicious prompts in images processed by AI systems before delivering them to a large language model. [...]

Malicious apps with +19M installs removed from Google Play because spreading Anatsa banking trojan and other malware

Security Affairs - 25 August 2025 18:56

Experts found 77 malicious Android apps with 19M+ installs on Google Play, spreading malware, including the Anatsa (TeaBot) banking trojan.

Phishing Campaign Uses UpCrypter in Fake Voicemail Emails to Deliver RAT Payloads

The Hacker News - 25 August 2025 22:34

Cybersecurity researchers have flagged a new phishing campaign that's using fake voicemails and purchase orders to deliver a malware loader called UpCrypter.

ClickFix Attack Tricks AI Summaries Into Pushing Malware

darkreading - 25 August 2025 20:32

Because instructions appear to come from AI-generated content summaries and not an external source, the victim is more likely to follow them without suspicion.