Scottish Cyber Coordination Centre

Daily Threat Bulletin

17 September 2025

Vulnerabilities

Apple Rolls Out iOS 26, macOS Tahoe 26 With Patches for Over 50 Vulnerabilities

SecurityWeek - 16 September 2025 09:44

Apple has announced major mobile and desktop platform releases and addressed an exploited bug in older platforms.

Apple backports fix for actively exploited CVE-2025-43300

Security Affairs - 17 September 2025 06:24

Apple has backported security patches released to address an actively exploited vulnerability tracked as CVE-2025-43300.

Chaos Mesh Critical GraphQL Flaws Enable RCE and Full Kubernetes Cluster Takeover

The Hacker News - 16 September 2025 22:53

Cybersecurity researchers have disclosed multiple critical security vulnerabilities in Chaos Mesh that, if successfully exploited, could lead to cluster takeover in Kubernetes environments.

Phoenix RowHammer Attack Bypasses Advanced DDR5 Memory Protections in 109 Seconds

The Hacker News - 16 September 2025 13:57

A team of academics from ETH Zürich and Google has discovered a new variant of a RowHammer attack targeting Double Data Rate 5 (DDR5) memory chips from South Korean semiconductor vendor SK Hynix.

ChatGPT's Calendar Integration Can Be Exploited to Steal Emails

SecurityWeek - 16 September 2025 11:51

Researchers show how a crafted calendar invite can trigger ChatGPT to exfiltrate sensitive emails.

Scottish Cyber Coordination Centre

Threat actors and malware

New FileFix attack uses steganography to drop StealC malware

BleepingComputer - 16 September 2025 09:00

A newly discovered FileFix social engineering attack impersonates Meta account suspension warnings to trick users into unknowingly installing the StealC infostealer malware.

Self-propagating supply chain attack hits 187 npm packages

BleepingComputer - 16 September 2025 13:46

Security researchers have identified at least 187 npm packages compromised in an ongoing supply chain attack. The coordinated worm-style campaign dubbed 'Shai-Hulud' started yesterday with the compromise of the @ctrl/tinycolor npm package, and has now expanded to CrowdStrike's npm namespace.

China-linked Mustang Panda deploys advanced SnakeDisk USB worm

Security Affairs - 16 September 2025 08:36

China-linked APT group Mustang Panda (aka Hive0154, Camaro Dragon, RedDelta or Bronze President) has been spotted using an updated version of the TONESHELL backdoor and a previously undocumented USB worm called SnakeDisk.

RaccoonO365 Phishing Network Dismantled as Microsoft, Cloudflare Take Down 338 Domains

The Hacker News - 17 September 2025 11:01

Microsoft's Digital Crimes Unit said it teamed up with Cloudflare to coordinate the seizure of 338 domains used by RaccoonO365, a financially motivated threat group that was behind a phishing-as-a-service (Phaas) toolkit used to steal more than 5,000 Microsoft 365 credentials from 94 countries since July 2024.

Google nukes 224 Android malware apps behind massive ad fraud campaign

BleepingComputer - 16 September 2025 14:20

A massive Android ad fraud operation dubbed "SlopAds" was disrupted after 224 malicious applications on Google Play were used to generate 2.3 billion ad requests per day.

Fifteen Ransomware Gangs "Retire," Future Unclear

Infosecurity Magazine - 16 September 2025 16:45

Fifteen ransomware groups have claimed shutdown on BreachForums; experts warn of rebrands and copycats.

Scottish Cyber Coordination Centre

UK incidents

Jaguar Land Rover extends shutdown after cyberattack by another week

BleepingComputer - 16 September 2025 10:08

Jaguar Land Rover (JLR) announced today that it will extend the production shutdown for another week, following a devastating cyberattack that impacted its systems at the end of August.