Scottish Cyber Coordination Centre

Daily Threat Bulletin

29 October 2025

Vulnerabilities

Chrome Zero-Day Actively Exploited in Attacks by Mem3nt0 mori

Infosecurity Magazine - 28 October 2025 17:00

A zero-day flaw in Chrome has been exploited by Mem3nt0 mori in Operation ForumTroll as part of a targeted espionage campaign

CVE-2025-62725: From “docker compose ps” to System Compromise

Security Boulevard - 28 October 2025 18:27

Docker Compose powers millions of workflows, from CI/CD runners and local development stacks to cloud workspaces and enterprise build pipelines. It’s trusted by developers as the friendly layer above Docker Engine that turns a few YAML lines into a running application.

Critical ASP.NET flaw hits QNAP NetBak PC Agent

Security Affairs - 28 October 2025 13:23

QNAP warns of critical ASP.NET flaw (CVE-2025-55315) in NetBak PC Agent, letting attackers hijack credentials or bypass security via HTTP smuggling.

CISA Adds Two Known Exploited Vulnerabilities to Catalog

CISA Advisories -

CISA has added two new vulnerabilities to its Known Exploited Vulnerabilities (KEV) Catalog, based on evidence of active exploitation.

CVE-2025-6204 Dassault Systèmes DELMIA Apriso Code Injection Vulnerability

CVE-2025-6205 Dassault Systèmes DELMIA Apriso Missing Authorization Vulnerability

Threat actors and malware

Aisuru botnet is behind record 20Tb/sec DDoS attacks

Security Affairs - 28 October 2025 21:22

In October 2025, the Aisuru Mirai-based IoT botnet launched massive DDoS attacks of over 20Tb/sec, mainly targeting online gaming, cybersecurity firm Netscout reports. The botnet uses residential proxies to reflect HTTPS DDoS attacks.

Scottish Cyber Coordination Centre

Qilin ransomware abuses WSL to run Linux encryptors in Windows

BleepingComputer - 28 October 2025 16:11

The Qilin ransomware operation was spotted executing Linux encryptors in Windows using Windows Subsystem for Linux (WSL) to evade detection by traditional security tools.

Google says reports of a Gmail breach have been greatly exaggerated

The Register - 28 October 2025 11:42

Ad and cloud biz rubbishes claims that 183 million accounts broken into Panic spread faster than a phishing email on Tuesday after claims of a massive Gmail breach hit the headlines – but Google says it's all nonsense.

New Android malware mimics human typing to evade detection, steal money

The Record from Recorded Future News - 28 October 2025 16:35

Researchers have discovered a new Android banking malware called Herodotus that evades detection by mimicking human behavior when remotely controlling infected devices.

Ransomware payments hit record low: only 23% Pay in Q3 2025

Security Affairs - 28 October 2025 10:21

Only 23% of ransomware victims paid in Q3 2025, the lowest ever, continuing a six-year decline in payment rates.