Scottish Cyber Coordination Centre

# Daily Threat Bulletin

8 April 2025

## Vulnerabilities

### Google fixes Android zero-days exploited in attacks, 60 other flaws

BleepingComputer - 07 April 2025 14:55

Google has released patches for 62 vulnerabilities in Android's April 2025 security update, including two zero-days exploited in targeted attacks. [...]

### U.S. CISA adds Ivanti Connect Secure, Policy Secure and ZTA Gateways flaw to its Known Exploited Vulnerabilities catalog

Security Affairs - 07 April 2025 20:39

U.S. Cybersecurity and Infrastructure Security Agency (CISA) adds Ivanti Connect Secure, Policy Secure and ZTA Gateways flaw to its Known Exploited Vulnerabilities catalog. The U.S. Cybersecurity and Infrastructure Security Agency (CISA) added an Apache Tomcat path equivalence vulnerability, tracked as CVE-2025-22457, to its Known Exploited Vulnerabilities (KEV) catalog.

### Google Releases Android Update to Patch Two Actively Exploited Vulnerabilities

The Hacker News - 08 April 2025 10:35

Google has shipped patches for 62 vulnerabilities, two of which it said have been exploited in the wild.

### NIST to Implement 'Deferred' Status to Dated Vulnerabilities

darkreading - 07 April 2025 20:00

The changes will go into effect over the next several days to reflect which CVEs are being prioritized in the National Vulnerability Database (NVD).

## Threat actors and malware

### The controversial case of the threat actor EncryptHub

Security Affairs - 07 April 2025 14:14

Microsoft credited controversial actor EncryptHub, a lone actor with ties to cybercrime, for reporting two Windows flaws. Microsoft credited the likely lone actor behind the EncryptHub alias (also known as SkorikARI) for reporting two Windows security flaws, highlighting a "conflicted" figure balancing ethical cybersecurity work with cybercriminal activity.

### PoisonSeed Campaign uses stolen email credentials to spread crypto seed scams and and empty wallets

Scottish Cyber Coordination Centre

Security Affairs - 07 April 2025 12:09

A campaign named PoisonSeed uses stolen CRM and bulk email credentials to send crypto seed scams, aiming to empty victims' digital wallets. Silent Push researchers warn of a malicious PoisonSeed campaign that uses stolen CRM and bulk email provider credentials to send crypto seed phrase spam. V

### CISA and FBI Warn Fast Flux is Powering Resilient Malware, C2, and Phishing Networks

The Hacker News - 07 April 2025 20:10

Cybersecurity agencies from Australia, Canada, New Zealand, and the United States have published a joint advisory about the risks associated with a technique called fast flux that has been adopted by threat actors to obscure a command-and-control (C2) channel.

### PoisonSeed Exploits CRM Accounts to Launch Cryptocurrency Seed Phrase Poisoning Attacks

The Hacker News - 07 April 2025 13:59

A malicious campaign dubbed PoisonSeed is leveraging compromised credentials associated with customer relationship management (CRM) tools and bulk email providers to send spam messages containing cryptocurrency seed phrases in an attempt to drain victims' digital wallets.

### ToddyCat APT Targets ESET Bug to Load Silent Malware

darkreading - 07 April 2025 21:43

Researchers found the threat actor attempting to use the now-patched flaw to load and execute a malicious dynamic link library on infected systems.

### That massive GitHub supply chain attack? It all started with a stolen SpotBugs token

The Register - 07 April 2025 21:11

But this mystery isn't over yet, Unit 42 opines That massive GitHub supply chain attack that spilled secrets from countless projects?

## UK related

### UK's attempt to keep details of Apple 'backdoor' case secret... denied

The Register - 07 April 2025 14:01

Last month's secret hearing comes to light Details of Apple's appeal against the UK's so-called "backdoor order" will now play out in public after the Home Office failed in its bid to keep them secret on national security grounds....