Scottish
Cyber
Coordination
Centre

Daily Threat Bulletin

16 September 2025

Vulnerabilities

Samsung Patches Zero-Day Exploited Against Android Users

SecurityWeek - 15 September 2025 09:08

Reported by Meta and WhatsApp, the vulnerability leads to remote code execution and was likely exploited by a spyware vendor.

Threat actors and malware

FBI Shares IoCs for Recent Salesforce Intrusion Campaigns

SecurityWeek - 15 September 2025 12:16

The cybercrime groups tracked as UNC6040 and UNC6395 have been extorting organizations after stealing data from their Salesforce instances.

New Phoenix attack bypasses Rowhammer defenses in DDR5 memory

BleepingComputer - 15 September 2025 15:01

Academic researchers have devised a new variant of Rowhammer attacks that bypass the latest protection mechanisms on DDR5 memory chips from SK Hynix. [...]

Hackers steal millions of Gucci, Balenciaga, and Alexander McQueen customer records

Security Affairs - 15 September 2025 23:27

Crooks stole personal data of millions of Gucci, Balenciaga, and Alexander McQueen customers: parent firm Kering confirmed the breach. Hackers stole private data of millions of Gucci, Balenciaga, and Alexander McQueen customers, including names, contacts, addresses, and spending details.

40 npm Packages Compromised in Supply Chain Attack Using bundle.js to Steal Credentials

The Hacker News - 16 September 2025 11:30

Cybersecurity researchers have flagged a fresh software supply chain attack targeting the npm registry that has affected more than 40 packages that belong to multiple maintainers.

HiddenGh0st, Winos and kkRAT Exploit SEO, GitHub Pages in Chinese Malware Attacks

The Hacker News - 15 September 2025 12:17

Chinese-speaking users are the target of a search engine optimization (SEO) poisoning campaign that uses fake software sites to distribute malware.”The attackers manipulated search rankings with SEO plugins and registered lookalike domains that closely mimicked legitimate software sites,” Fortinet FortiGuard Labs researcher Pei Han Liao said.

Threat Group Scattered Lapsus$ Hunters Says It’s Shutting Down

Security Boulevard - 15 September 2025 18:13

The bad actors behind the Scattered Lapsus$ Hunters threat group say they are shutting down operations and retiring, but cybersecurity pros say law enforcement pressure is a key reason for the decision and that the hackers will likely form new cybercrime operations.

Phishing Campaigns Drop RMM Tools for Remote Access

Infosecurity Magazine - 15 September 2025 09:30

Threat actors are using multiple lures to trick users into installing RMM tools

UK related

Google owner reveals £5bn AI investment in UK ahead of Trump visit

BBC News - 16 September 2025 05:00

Google’s President and Chief Investment Officer Ruth Porat tells the BBC there are “profound opportunities in the UK”.