Scottish Cyber Coordination Centre

Daily Threat Bulletin

30 June 2025

Vulnerabilities

‘CitrixBleed 2’ Shows Signs of Active Exploitation

darkreading - 27 June 2025 19:50

If exploited, the critical vulnerability allows attackers to maintain access for longer periods of time than the original CitrixBleed flaw, all while remaining undetected.

Taking over millions of developers exploiting an Open VSX Registry flaw

Security Affairs - 27 June 2025 20:37

A critical flaw in Open VSX Registry could let attackers hijack the VS Code extension hub, exposing millions of developers to supply chain attacks.

MOVEit Transfer Faces Increased Threats as Scanning Surges and CVE Flaws Are Targeted

The Hacker News - 27 June 2025 14:13

Threat intelligence firm GreyNoise is warning of a “notable surge” in scanning activity targeting Progress MOVEit Transfer systems starting May 27, 2025 - suggesting that attackers may be preparing for another mass exploitation campaign or probing for unpatched systems.

Bluetooth flaws could let hackers spy through your microphone

BleepingComputer - 29 June 2025 13:03

Vulnerabilities affecting a Bluetooth chipset present in more than two dozen audio devices from ten vendors can be exploited for eavesdropping or stealing sensitive information.

Vulnerability Exposed All Open VSX Repositories to Takeover

SecurityWeek - 27 June 2025 09:18

A vulnerability in the extension publishing mechanism of Open VSX could have allowed attackers to tamper with any repository.

Threat actors and malware

Scattered Spider hackers shift focus to aviation, transportation firms

BleepingComputer - 27 June 2025 15:20

Hackers associated with Scattered Spider tactics have expanded their targeting to the aviation and transportation industries after previously attacking insurance and retail sectors.

Scottish Cyber Coordination Centre

GIFTEDCROOK Malware Evolves: From Browser Stealer to Intelligence-Gathering Tool

The Hacker News - 28 June 2025 14:28

The threat actor behind the GIFTEDCROOK malware has made significant updates to turn the malicious program from a basic browser data stealer to a potent intelligence-gathering tool.

LapDogs: China-nexus hackers Hijack 1,000+ SOHO devices for espionage

Security Affairs - 28 June 2025 14:29

Security researchers have uncovered a cyber espionage campaign, dubbed LapDogs, involving over 1,000 hacked SOHO (small office/home office) devices.

Chinese Group Silver Fox Uses Fake Websites to Deliver Sainbox RAT and Hidden Rootkit

The Hacker News - 27 June 2025 16:55

A new campaign has been observed leveraging fake websites advertising popular software such as WPS Office, Sogou, and DeepSeek to deliver Sainbox RAT and the open-source Hidden rootkit.