Scottish Cyber Coordination Centre

Daily Threat Bulletin

20 May 2026

Vulnerabilities

Max-severity flaw in ChromaDB for AI apps allows server hijacking

BleepingComputer - 19 May 2026 19:25

A max-severity vulnerability in the latest Python FastAPI version of the ChromaDB project allows unauthenticated attackers to run arbitrary code on exposed servers.

Critical Microsoft Vulnerabilities Doubled: From Exposure to Escalation

BleepingComputer - 19 May 2026 11:00

Microsoft's total vulnerability count stayed steady in 2025, but critical flaws surged year over year. BeyondTrust breaks down why attackers are increasingly focused on privilege escalation and identity abuse.

DirtyDecrypt PoC Released for Linux Kernel CVE-2026-31635 LPE Vulnerability

The Hacker News - 19 May 2026 21:26

Proof-of-concept (PoC) exploit code has now been released for a recently patched security flaw in the Linux kernel that could allow for local privilege escalation (LPE). Dubbed DirtyDecrypt (aka DirtyCBC), the vulnerability was discovered and reported by the Zellic and V12 security team on May 9, 2026.

Drupal to Patch Highly Critical Vulnerability at Risk of Quick Exploitation

SecurityWeek - 19 May 2026 17:22

Drupal says attackers may develop an exploit for the vulnerability within hours or days.

Threat actors and malware

GitHub investigates internal repositories breach claimed by TeamPCP

BleepingComputer - 20 May 2026 02:08

GitHub is investigating a breach of its internal repositories after the TeamPCP hacker group claimed to have accessed approximately 4,000 repositories containing private code.

New Shai-Hulud malware wave compromises 600 npm packages

BleepingComputer - 19 May 2026 11:30

Threat actors earlier today published more than 600 malicious packages to the Node Package Manager (npm) index as part of a new Shai-Hulud supply-chain campaign.

Scottish Cyber Coordination Centre

Microsoft Disrupts Malware-Signing Service Run by 'Fox Tempest'

SecurityWeek - 19 May 2026 17:06

Fox Tempest provides a service that cybercriminals use to distribute ransomware and other malware disguised as legitimate software.

Legacy Windows Tool MSHTA Fuels Surge in Silent Malware Attacks

SecurityWeek - 19 May 2026 14:00

Attackers are increasingly abusing Microsoft's decades-old MSHTA utility to stealthily deliver stealers, loaders, and persistent malware through phishing, fake software downloads, and LOLBIN-based attack chains.