Scottish
Cyber
Coordination
Centre

Daily Threat Bulletin

30 July 2025

Vulnerabilities

Hackers exploit SAP NetWeaver bug to deploy Linux Auto-Color malware

BleepingComputer - 29 July 2025 13:10

Hackers were spotted exploiting a critical SAP NetWeaver vulnerability tracked as CVE-2025-31324 to deploy the Auto-Color Linux malware in a cyberattack on a U.S.-based chemicals company.

Wiz Uncovers Critical Access Bypass Flaw in AI-Powered Vibe Coding Platform Base44

The Hacker News - 29 July 2025 22:08

Cybersecurity researchers have disclosed a now-patched critical security flaw in a popular vibe coding platform called Base44 that could allow unauthorized access to private applications built by its users.

Lenovo Firmware Vulnerabilities Allow Persistent Implant Deployment

SecurityWeek - 29 July 2025 18:00

Vulnerabilities discovered by Binarly in Lenovo devices allow privilege escalation, code execution, and security bypass.

Threat actors and malware

PyPI Warns of Ongoing Phishing Campaign Using Fake Verification Emails and Lookalike Domain

The Hacker News - 29 July 2025 20:57

The maintainers of the Python Package Index (PyPI) repository have issued a warning about an ongoing phishing attack that’s targeting users in an attempt to redirect them to fake PyPI sites.

Ransomware Statistics: Updates on Ransoms, Attacks and Active Groups

Security Magazine - 29 July 2025 09:00

Data reveals global ransomware trends for the first half of 2025.

GOLD BLADE remote DLL sideloading attack deploys RedLoader

Threat Research – Sophos News - 29 July 2025 17:39

Attacks surged in July 2025 after the threat group updated its process to combine malicious LNK files and a recycled WebDAV technique.

Nimble 'Gunra' Ransomware Evolves With Linux Variant

darkreading - 29 July 2025 21:17

The emerging cybercriminal gang, which initially targeted Microsoft Windows systems, is looking to go cross-platform using sophisticated, multithread encryption.