Scottish
Cyber
Coordination
Centre

Daily Threat Bulletin

12 August 2025

Vulnerabilities

Details emerge on WinRAR zero-day attacks that infected PCs with malware

BleepingComputer - 11 August 2025 15:05

Researchers have released a report detailing how a recent WinRAR path traversal vulnerability tracked as CVE-2025-8088 was exploited in zero-day attacks by the Russian 'RomCom' hacking group to drop different malware payloads. [...]

Smart Buses flaws expose vehicles to tracking, control, and spying

Security Affairs - 11 August 2025 09:40

Researchers showed how hackers can exploit flaws in a bus' onboard and remote systems for tracking, control and spying. Researchers Chiao-Lin 'Steven Meow' Yu of Trend Micro Taiwan and Kai-Ching 'Keniver' Wang of CHT Security, found that vulnerabilities in smart bus systems could let hackers remotely track, control, or spy on vehicles.

New TETRA Radio Encryption Flaws Expose Law Enforcement Communications

The Hacker News - 11 August 2025 23:02

Cybersecurity researchers have discovered a fresh set of security issues in the Terrestrial Trunked Radio (TETRA) communications protocol, including in its proprietary end-to-end encryption (E2EE) mechanism that exposes the system to replay and brute-force attacks, and even decrypt encrypted traffic.

Researchers Spot Surge in Erlang/OTP SSH RCE Exploits, 70% Target OT Firewalls

The Hacker News - 11 August 2025 21:38

Malicious actors have been observed exploiting a now-patched critical security flaw impacting Erlang/Open Telecom Platform (OTP) SSH as early as beginning of May 2025, with about 70% of detections originating from firewalls protecting operational technology (OT) networks.

Threat actors and malware

The Rise of Native Phishing: Microsoft 365 Apps Abused in Attacks

BleepingComputer - 11 August 2025 12:17

Native phishing turns trusted tools into attack delivery systems. Varonis shows how attackers weaponize Microsoft 365 apps, like OneNote & OneDrive, to send convincing internal lures and how to spot them before they spread. [...]

UK related

UK Red Teamers “Deeply Skeptical” of AI

Infosecurity Magazine - 11 August 2025 09:25

Commercial red team experts believe AI’s current impact on cyber is overstated