Scottish Cyber Coordination Centre

Daily Threat Bulletin

4 September 2025

Threat actors and malware

SaaS giant Workiva discloses data breach after Salesforce attack

BleepingComputer - 03 September 2025 13:40

Workiva, a leading cloud-based SaaS (Software as a Service) provider, notified its customers that attackers who gained access to a third-party customer relationship management (CRM) system stole some of their data. [...]

Hackers use new HexStrike-AI tool to rapidly exploit n-day flaws

BleepingComputer - 03 September 2025 15:03

Hackers are increasingly using a new AI-powered offensive security framework called HexStrike-AI in real attacks to exploit newly disclosed n-day flaws. [...]

Android droppers evolved into versatile tools to spread malware

Security Affairs - 03 September 2025 10:41

Android droppers now spread banking trojans, SMS stealers, and spyware, disguised as government or banking apps in India and Asia. ThreatFabric researchers warn of a shift in Android malware: dropper apps now deliver not just banking trojans, but also SMS stealers and spyware, mainly in Asia. Google's Pilot Program enhances Play Protect by scanning Android [...]

Jaguar Land Rover shuts down systems after cyberattack, no evidence of customer data theft

Security Affairs - 03 September 2025 09:08

Jaguar Land Rover shut down systems after a cyberattack, disrupting production and retail, but says customer data likely remains safe. Jaguar Land Rover shut down systems to mitigate a cyberattack that disrupted production and retail operations. The attack occurred over the weekend, and it also impacted systems at the Solihull production plant. UK dealers reported [...]

Iranian Hackers Exploit 100+ Embassy Email Accounts in Global Phishing Targeting Diplomats

The Hacker News - 03 September 2025 17:00

An Iran-nexus group has been linked to a "coordinated" and "multi-wave" spear-phishing campaign targeting the embassies and consulates in Europe and other regions across the world.The activity has been attributed by Israeli cybersecurity company Dream to Iranian-aligned operators connected to broader offensive cyber activity undertaken by a group known as Homeland Justice."Emails were sent to

Scottish Cyber Coordination Centre

Vulnerabilities

Google fixes actively exploited Android flaws in September update

BleepingComputer - 03 September 2025 11:14

Google has released the September 2025 security update for Android devices, addressing a total of 84 vulnerabilities, including two actively exploited flaws. [...]

U.S. CISA adds WhatsApp, and TP-link flaws to its Known Exploited Vulnerabilities catalog

Security Affairs - 03 September 2025 13:09

U.S. Cybersecurity and Infrastructure Security Agency (CISA) adds WhatsApp, and TP-link flaws to its Known Exploited Vulnerabilities catalog. The U.S. Cybersecurity and Infrastructure Security Agency (CISA) added WhatsApp, and TP-link flaws to its Known Exploited Vulnerabilities (KEV) catalog. Below are the descriptions for these flaws: CVE-2020-24363 (CVSS 8.8) is a missing authentication flaw in TP-Link TL-WA855RE [...]

WhatsApp Bug Anchors Targeted Zero-Click iPhone Attacks

darkreading - 03 September 2025 14:24

A "sophisticated" attack that also exploits an Apple zero-day flaw is targeting a specific group of iPhone users, potentially with spyware.

UK related

M&S hackers claim to be behind Jaguar Land Rover cyber attack

BBC News - 03 September 2025 18:08

The hack has caused severe disruption at manufacturing plants globally, with some staff told not to come into work.