Scottish Cyber Coordination Centre

Daily Threat Bulletin

3 September 2025

Vulnerabilities

Frostbyte10 bugs put thousands of refrigerators at major grocery chains at risk

The Register - 02 September 2025 10:00

Major flaws uncovered in Copeland controllers: Patch now Ten vulnerabilities in Copeland controllers, which are found in thousands of devices used by the world's largest supermarket chains and cold storage companies, could have allowed miscreants to manipulate temperatures and spoil food and medicine, leading to massive supply-chain disruptions....

Sangoma Patches Critical Zero-Day Exploited to Hack FreePBX Servers

SecurityWeek - 02 September 2025 19:11

Tracked as CVE-2025-57819 (CVSS score of 10/10), the bug is described as an insufficient sanitization of user-supplied data. The post Sangoma Patches Critical Zero-Day Exploited to Hack FreePBX Servers appeared first on SecurityWeek.

WhatsApp, Apple warn of highly targeted attacks with zero-day vulnerability

The Record from Recorded Future News - 02 September 2025 16:47

CISA Adds Two Known Exploited Vulnerabilities to Catalog

CISA Advisories -

CISA has added two new vulnerabilities to its Known Exploited Vulnerabilities (KEV) Catalog, based on evidence of active exploitation: CVE-2020-24363 TP-link TL-WA855RE Missing Authentication for Critical Function Vulnerability; CVE-2025-55177 Meta Platforms WhatsApp Incorrect Authorization Vulnerability.

Threat actors and malware

Cloudflare blocks largest recorded DDoS attack peaking at 11.5 Tbps

BleepingComputer - 02 September 2025 12:52

Internet infrastructure company Cloudflare said it recently blocked the largest recorded volumetric distributed denial-of-service (DDoS) attack, which peaked at 11.5 terabits per second (Tbps). [...]

Jaguar Land Rover says cyberattack 'severely disrupted' production

BleepingComputer - 02 September 2025 11:23

Jaguar Land Rover (JLR) announced that a cyberattack forced the company to shut down certain systems as part of the mitigation effort. [...]

Lazarus Group Expands Malware Arsenal With PondRAT, ThemeForestRAT, and RemotePE

The Hacker News - 02 September 2025 23:09

The North Korea-linked threat actor known as the Lazarus Group has been attributed to a social engineering campaign that distributes three different pieces of cross-platform malware called PondRAT, ThemeForestRAT, and RemotePE.

Malicious npm Package nodejs-smtp Mimics Nodemailer, Targets Atomic and Exodus Wallets

The Hacker News - 02 September 2025 11:10

Cybersecurity researchers have discovered a malicious npm package that comes with stealthy features to inject malicious code into desktop apps for cryptocurrency wallets like Atomic and Exodus on Windows systems.

Amazon Stymies APT29 Credential Theft Campaign

darkreading - 02 September 2025 21:25

A group linked to Russian intelligence services redirected victims to fake Cloudflare verification pages and exploited Microsoft's device code authentication flow.

UK related

UK NCSC Supports Public Disclosure for AI Safeguard Bypass Threats

Infosecurity Magazine - 02 September 2025 10:45

The UK National Cyber Security Centre thinks public disclosure programs could help mitigate AI safety threats