Scottish Cyber Coordination Centre

Daily Threat Bulletin

22 October 2025

Vulnerabilities

TP-Link Patches Four Omada Gateway Flaws, Two Allow Remote Code Execution

The Hacker News - 22 October 2025 11:08

TP-Link has released security updates to address four security flaws impacting Omada gateway devices, including two critical bugs that could result in arbitrary code execution.

Oracle October 2025 Critical Patch Update Addresses 170 CVEs

Security Boulevard - 21 October 2025 21:42

On October 21, Oracle released its Critical Patch Update (CPU) for October 2025, the fourth and final quarterly update of the year. This CPU contains fixes for 170 unique CVEs in 374 security updates across 29 Oracle product families.

Over 73,000 WatchGuard Firebox Devices Impacted by Recent Critical Flaw

SecurityWeek - 21 October 2025 11:00

Affecting the Fireware OS iked process, the vulnerability can lead to remote code execution and does not require authentication.

Cursor, Windsurf IDEs riddled with 94+ n-day Chromium vulnerabilities

BleepingComputer - 21 October 2025 16:00

The latest releases of Cursor and Windsurf integrated development environments are vulnerable to more than 94 known and patched security issues in the Chromium browser and the V8 JavaScript engine.

Hackers exploit 34 zero-days on first day of Pwn2Own Ireland

BleepingComputer - 21 October 2025 14:39

On the first day of Pwn2Own Ireland 2025, security researchers exploited 34 unique zero-days and collected $522,500 in cash awards.

Threat actors and malware

Russia-linked COLDRIVER speeds up malware evolution after LOSTKEYS exposure

Security Affairs - 22 October 2025 07:06

The Russia-linked hacking group COLDRIVER has been quickly upgrading its malware since May 2025, when its LOSTKEYS malware was exposed.

China-Linked Salt Typhoon breaches European Telecom via Citrix exploit

Security Affairs - 21 October 2025 12:27

A European telecom firm was targeted in July 2025 by China-linked APT group Salt Typhoon (also known as Earth Estries, FamousSparrow, GhostEmperor, UNC5807, RedMike)), which exploited a Citrix NetScaler Gateway to gain initial access.

Russian hackers evolve malware pushed in “I am not a robot” captchas

BleepingComputer - 21 October 2025 12:13

The Russian state-backed Star Blizzard hacker group has ramped up operations with new, constantly evolving malware families (NoRobot, MaybeRobot) deployed in complex delivery chains that start with ClickFix social engineering attacks.

PolarEdge Targets Cisco, ASUS, QNAP, Synology Routers in Expanding Botnet Campaign

The Hacker News - 21 October 2025 20:17

Cybersecurity researchers have shed light on the inner workings of a botnet malware called PolarEdge. PolarEdge was first documented by Sekoia in February 2025, attributing it to a campaign targeting routers from Cisco, ASUS, QNAP, and Synology with the goal of corralling them into a network for an as-yet-undetermined purpose.

Lumma Stealer Developers Doxxed in Underground Rival Cybercrime Campaign

Infosecurity Magazine - 21 October 2025 09:00

Lumma Stealer operators allegedly exposed in underground doxxing campaign, with sensitive details leaked by rival cybercriminals.