Scottish Cyber Coordination Centre

Daily Threat Bulletin

6 May 2025

Vulnerabilities

Microsoft silently fixes Start menu bug affecting Windows 10 PCs

BleepingComputer - 05 May 2025 08:48

Microsoft has silently fixed an issue that broke Start Menu jump lists for all apps on systems running Windows 10, version 22H2. [...]

Google Fixes Actively Exploited Android System Flaw in May 2025 Security Update

The Hacker News - 06 May 2025 12:16

Google has released its monthly security updates for Android with fixes for 46 security flaws, including one vulnerability that it said has been exploited in the wild.The vulnerability in question is CVE-2025-27363 (CVSS score: 8.1), a high-severity flaw in the System component that could lead to local code execution without requiring any additional execution privileges

Wormable AirPlay Flaws Enable Zero-Click RCE on Apple Devices via Public Wi-Fi

The Hacker News - 05 May 2025 23:36

Cybersecurity researchers have disclosed a series of now-patched security vulnerabilities in Apple's AirPlay protocol that, if successfully exploited, could enable an attacker to take over susceptible devices supporting the proprietary wireless technology.The shortcomings have been collectively codenamed AirBorne by Israeli cybersecurity company Oligo.

Critical Commvault Vulnerability in Attacker Crosshairs

SecurityWeek - 05 May 2025 13:17

CISA has flagged a critical-severity Commvault vulnerability as exploited one week after technical details were released.

PoC Published for Exploited SonicWall Vulnerabilities

SecurityWeek - 05 May 2025 10:55

PoC code targeting two exploited SonicWall flaws was published just CISA added them to the KEV catalog.

CISA Adds One Known Exploited Vulnerability to Catalog

CISA Advisories -

CISA has added one new vulnerability to its Known Exploited Vulnerabilities Catalog, based on evidence of active exploitation.CVE-2025-3248 Langflow Missing Authentication vulnerability.

Scottish Cyber Coordination Centre

Threat actors and malware

Luna Moth extortion hackers pose as IT help desks to breach US firms

BleepingComputer - 05 May 2025 19:19

The data-theft extortion group known as Luna Moth, aka Silent Ransom Group, has ramped up callback phishing campaigns in attacks on legal and financial institutions in the United States. [...]

New "Bring Your Own Installer" EDR bypass used in ransomware attack

BleepingComputer - 05 May 2025 17:28

A new "Bring Your Own Installer" EDR bypass technique is exploited in attacks to bypass SentinelOne's tamper protection feature, allowing threat actors to disable endpoint detection and response (EDR) agents to install the Babuk ransomware. [...]

A hacker stole data from TeleMessage, the firm that sells modified versions of Signal to the U.S. gov

Security Affairs - 05 May 2025 13:06

A hacker stole data from TeleMessage, exposing messages from its modified Signal, WhatsApp, and other apps sold to the U.S. government. A hacker stole customer data from TeleMessage, an Israeli firm selling modified versions of popular messaging apps, such as Signal and WhatsApp, to the U.S. government.

Experts shared up-to-date C2 domains and other artifacts related to recent MintsLoader attacks

Security Affairs - 05 May 2025 12:24

MintsLoader is a malware loader delivering the GhostWeaver RAT via a multi-stage chain using obfuscated JavaScript and PowerShell. Recorded Future researchers observed MintsLoader delivering payloads like GhostWeaver via obfuscated scripts, evading detection with sandbox/VM checks, and uses DGA and HTTP C2.

Ransomware Attacks Fall in April Amid RansomHub Outage

Infosecurity Magazine - 05 May 2025 09:15

Comparitech observed a significant decline in ransomware attacks in April, partly as a result of the RansomHub gang "going dark"

UK related

UK shares security tips after major retail cyberattacks

BleepingComputer - 05 May 2025 12:19

Following three high-profile cyberattacks impacting major UK retailers, the country's National Cyber Security Centre (NCSC) has published guidance that all companies are advised to follow to strengthen their cybersecurity defenses. [...]

Scottish Cyber Coordination Centre

[Harrods' Cyberattack: Cybersecurity Leaders Weigh In]

Security Magazine - 06 May 2025 02:00

Harrods experienced a cyberattack, and cybersecurity leaders are sharing their insights.