Scottish
Cyber
Coordination
Centre

Daily Threat Bulletin

2 April 2025

Vulnerabilities

CrushFTP CVE-2025-2825 flaw actively exploited in the wild

Security Affairs - 01 April 2025 15:09

Threat actors are exploiting a critical authentication bypass vulnerability, tracked as CVE-2025-2825, in the CrushFTP file transfer software. Attackers are using exploits based on publicly available proof-of-concept exploit code.

Critical Vulnerability Found in Canon Printer Drivers

SecurityWeek - 01 April 2025 12:50

Microsoft’s offensive security team warned Canon about a critical code execution vulnerability in printer drivers.

Google ‘ImageRunner’ Bug Enabled Privilege Escalation

darkreading - 01 April 2025 15:00

Tenable released details of a Google Cloud Run flaw that prior to remediation allowed a threat actor to escalate privileges.

WP Ultimate CSV Importer Flaws Expose 20,000 Websites to Attacks

Infosecurity Magazine - 01 April 2025 16:30

WP Ultimate CSV Importer flaws expose 20,000 websites to attacks enabling attackers to achieve full site compromise.

Apple backports zero-day patches to older iPhones and Macs

BleepingComputer - 01 April 2025 10:35

Apple has released security updates that backport fixes for actively exploited vulnerabilities that were exploited as zero-days to older versions of its operating systems.

Threat actors and malware

Nearly 24,000 IPs Target PAN-OS GlobalProtect in Coordinated Login Scan Campaign

The Hacker News - 01 April 2025 17:47

Cybersecurity researchers are warning of a spike in suspicious login scanning activity targeting Palo Alto Networks PAN-OS GlobalProtect gateways, with nearly 24,000 unique IP addresses attempting to access these portals.

New Malware Loaders Use Call Stack Spoofing, GitHub C2, and .NET Reactor for Stealth

The Hacker News - 02 April 2025 12:25

Cybersecurity researchers have discovered an updated version of a malware loader called Hijack Loader that implements new features to evade detection and establish persistence on compromised systems.

China-Linked Earth Alux Uses VARGEIT and COBEACON in Multi-Stage Cyber Intrusions

The Hacker News - 01 April 2025 17:33

Cybersecurity researchers have shed light on a new China-linked threat actor called Earth Alux that has targeted various key sectors such as government, technology, logistics, manufacturing, telecommunications, IT services, and retail.

Qilin affiliates spear-phish MSP ScreenConnect admin, targeting customers downstream

Threat Research – Sophos News - 01 April 2025 11:30

Attack matches three-year long pattern of ScreenConnect attacks tracked by Sophos MDR as STAC4365.

UK specific

Cyber Security and Resilience Bill Will Apply to 1000 UK Firms

Infosecurity Magazine - 01 April 2025 09:45

A thousand UK service providers will be expected to comply with the forthcoming Cyber Security and Resilience Bill.