Scottish
Cyber
Coordination
Centre

Daily threat bulletin

5 February 2025

Vulnerabilities

Zyxel won’t patch newly exploited flaws in end-of-life routers

BleepingComputer - 04 February 2025 17:22

Zyxel has issued a security advisory about actively exploited flaws in CPE Series devices, warning that it has no plans to issue fixing patches and urging users to move to actively supported models. [...]

7-Zip MotW bypass exploited in zero-day attacks against Ukraine

BleepingComputer - 04 February 2025 10:43

A 7-Zip vulnerability allowing attackers to bypass the Mark of the Web (MotW) Windows security feature was exploited by Russian hackers as a zero-day since September 2024. [...]

Netgear urges users to upgrade two flaws impacting WiFi router models

Security Affairs - 04 February 2025 23:24

Netgear disclosed two critical flaws impacting multiple WiFi router models and urges customers to address them. Netgear addressed two critical vulnerabilities, internally tracked as PSV-2023-0039 and PSV-2021-0117, impacting multiple WiFi router models and urged customers to install the latest firmware.

AMD fixed a flaw that allowed to load malicious microcode

Security Affairs - 04 February 2025 15:49

AMD released security patches to fix a flaw that could bypass SEV protection, letting attackers load malicious microcode. Researchers from Google disclosed an improper signature verification vulnerability, tracked as CVE-2024-56161 (CVSS score of 7.2), in AMD’s Secure Encrypted Virtualization (SEV).

CISA Adds Four Actively Exploited Vulnerabilities to KEV Catalog, Urges Fixes by Feb 25

The Hacker News - 05 February 2025 11:35

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) on Tuesday added four security flaws to its Known Exploited Vulnerabilities (KEV) catalog, citing evidence of active exploitation in the wild.T

Malicious Go Package Exploits Module Mirror Caching for Persistent Remote Access

The Hacker News - 04 February 2025 20:46

Cybersecurity researchers have called attention to a software supply chain attack targeting the Go ecosystem that involves a malicious package capable of granting the adversary remote access to infected systems.

Google Patches 47 Android Security Flaws, Including Actively Exploited CVE-2024-53104

The Hacker News - 04 February 2025 11:21

Google has shipped patches to address 47 security flaws in its Android operating system, including one it said has come under active exploitation in the wild.The vulnerability in question is CVE-2024-53104 (CVSS score: 7.8), which has been described as a case of privilege escalation in a kernel component known as the USB Video Class (UVC) driver.

Microsoft SharePoint Connector Flaw Could've Enabled Credential Theft Across Power Platform

The Hacker News - 04 February 2025 10:59

Cybersecurity researchers have disclosed details of a now-patched vulnerability impacting the Microsoft SharePoint connector on Power Platform that, if successfully exploited, could allow threat actors to harvest a user's credentials and stage follow-on attacks.

Threat actors and malware

Chinese cyberspies use new SSH backdoor in network device hacks

BleepingComputer - 04 February 2025 13:39

A Chinese hacking group is hijacking the SSH daemon on network appliances by injecting malware into the process for persistent access and covert operations. [...]

Russian Cybercrime Groups Exploiting 7-Zip Flaw to Bypass Windows MotW Protections

The Hacker News - 04 February 2025 18:58

A recently patched security vulnerability in the 7-Zip archiver tool was exploited in the wild to deliver the SmokeLoader malware.

North Korean Hackers Deploy FERRET Malware via Fake Job Interviews on macOS

The Hacker News - 04 February 2025 18:41

The North Korean threat actors behind the Contagious Interview campaign have been observed delivering a collection of Apple macOS malware strains dubbed FERRET as part of a supposed job interview process.

Credential Theft Becomes Cybercriminals' Favorite Target

darkreading - 04 February 2025 23:15

Researchers measured a threefold increase in credential stealing between 2023 and 2024, with more than 11.3 million such thefts last year.

22 New Mac Malware Families Seen in 2024

SecurityWeek - 04 February 2025 18:01

Nearly two dozen new macOS malware families were observed in 2024, including stealers, backdoors, downloaders and ransomware.

UK related

Cyberattack on NHS causes hospitals to miss cancer care targets

The Register - 04 February 2025 12:44

Healthcare chiefs say impact will persist for months NHS execs admit that last year’s cyberattack on hospitals in Wirral, northwest England, continues to “significantly” impact waiting times for cancer treatments, and suspect this will last for “months.”...