Scottish Cyber Coordination Centre

Daily Threat Bulletin

11 August 2025

Vulnerabilities

WinRAR zero-day exploited to plant malware on archive extraction

BleepingComputer - 08 August 2025 17:42

A recently fixed WinRAR vulnerability tracked as CVE-2025-8088 was exploited as a zero-day in phishing attacks to install the RomCom malware. [...]

BadCam: Linux-based Lenovo webcam bugs enable BadUSB attacks

Security Affairs - 10 August 2025 08:10

Lenovo webcam flaws, dubbed BadCam, let attackers turn them into BadUSB devices to inject keystrokes and launch OS-independent attacks.

New Win-DDoS Flaws Let Attackers Turn Public Domain Controllers into DDoS Botnet via RPC, LDAP

The Hacker News - 11 August 2025 02:00

A novel attack technique could be weaponized to rope thousands of public domain controllers (DCs) around the world to create a malicious botnet and use it to conduct powerful distributed denial-of-service (DDoS) attacks.

Researchers Detail Windows EPM Poisoning Exploit Chain Leading to Domain Privilege Escalation

The Hacker News - 10 August 2025 19:01

Cybersecurity researchers have presented new findings related to a now-patched security issue in Microsoft's Windows Remote Procedure Call (RPC) communication protocol that could be abused by an attacker to conduct spoofing attacks and impersonate a known server.The vulnerability, tracked as CVE-2025-49760 (CVSS score: 3.5), has been described by the tech giant as a Windows Storage spoofing bug.

CyberArk and HashiCorp Flaws Enable Remote Vault Takeover Without Credentials

The Hacker News - 09 August 2025 11:45

Cybersecurity researchers have discovered over a dozen vulnerabilities in enterprise secure vaults from CyberArk and HashiCorp that, if successfully exploited, can allow remote attackers to crack open corporate identity systems and extract enterprise secrets and tokens from them.

Trend Micro offers weak workaround for already-exploited critical vuln in management console

Scottish Cyber Coordination Centre

The Register - 10 August 2025 23:39

Threat actors and malware

Google confirms Salesforce CRM breach, faces extortion threat

Security Affairs - 10 August 2025 18:37

Google disclosed a Salesforce Customer Relationship Management (CRM) breach exposing data of some prospective Google Ads customers.

SonicWall dismisses zero-day fears after Ransomware probe

Security Affairs - 08 August 2025 08:03

SonicWall found no evidence of a new vulnerability after probing reports of a zero-day used in ransomware attacks.

Researchers Reveal ReVault Attack Targeting Dell ControlVault3 Firmware in 100+ Laptop Models

The Hacker News - 10 August 2025 01:25

Cybersecurity researchers have uncovered multiple security flaws in Dell's ControlVault3 firmware and its associated Windows APIs that could have been abused by attackers to bypass Windows login, extract cryptographic keys, as well as maintain access even after a fresh operating system install by deploying undetectable malicious implants into the firmware.

Leaked Credentials Up 160%: What Attackers Are Doing With Them

The Hacker News - 08 August 2025 17:30

When an organization's credentials are leaked, the immediate consequences are rarely visible—but the long-term impact is far-reaching. Far from the cloak-and-dagger tactics seen in fiction, many real-world cyber breaches begin with something deceptively simple: a username and password.

CISA Releases a Malware and Forensic Analysis Platform

Security Magazine - 08 August 2025 12:00

CISA has released a malware and forensic analysis platform.

Ransomware Attacks Fall by Almost Half in Q2

darkreading - 08 August 2025 17:49

UK related

Scottish Cyber Coordination Centre

UK proxy traffic surges as users consider VPN alternatives amid Online Safety Act

The Register - 08 August 2025 10:45

It's 'more than a temporary trend,' Decodo claims Amid the furor around surging VPN usage in the UK, many users are eyeing proxies as a potential alternative to the technology....