Scottish Cyber Coordination Centre

Daily threat bulletin

23 October 2024

Vulnerabilities

Windows 10 KB5045594 update fixes multi-function printer bugs

BleepingComputer - 22 October 2024 17:50

Microsoft has released the optional KB5045594 preview cumulative update for Windows 10 22H2 with fixes for problems printing to multi-function printers and other issues. [...]

Exploit released for new Windows Server "WinReg" NTLM Relay attack

BleepingComputer - 22 October 2024 14:26

Proof-of-concept exploit code is now public for a vulnerability in Microsoft's Remote Registry client that could be used to take control of a Windows domain by downgrading the security of the authentication process. [...]

VMware Releases vCenter Server Update to Fix Critical RCE Vulnerability

The Hacker News - 22 October 2024 13:33

VMware has released software updates to address an already patched security flaw in vCenter Server that could pave the way for remote code execution.The vulnerability, tracked as CVE-2024-38812 (CVSS score: 9.8), concerns a case of heap-overflow vulnerability in the implementation of the DCE/RPC protocol.

Critical Vulnerabilities Expose mbNET.mini, Helmholz Industrial Routers to Attacks

SecurityWeek - 22 October 2024 12:55

Critical and high-severity vulnerabilities that can lead to full device compromise have been found in mbNET.mini and Helmholz industrial routers.

Samsung zero-day flaw actively exploited in the wild

Security Affairs - 22 October 2024 16:41

Google's Threat Analysis Group (TAG) researchers warn of a Samsung zero-day vulnerability that is exploited in the wild. Google's Threat Analysis Group (TAG) warns of a Samsung zero-day vulnerability, tracked as CVE-2024-44068 (CVSS score of 8.1).

OPA for Windows Vulnerability Exposes NTLM Hashes

darkreading - 22 October 2024 22:10

The vulnerability affects all versions prior to v0.68.0 and highlights the risks organizations assume when consuming open source software and code.

Scottish Cyber Coordination Centre

Threat actors and malware

Experts warn of a new wave of Bumblebee malware attacks

Security Affairs - 22 October 2024 14:13

Experts warn of a new wave of attacks involving the Bumblebee malware, months after Europol's 'Operation Endgame' that disrupted its operations in May. The Bumblebee malware loader has resurfaced in new attacks, four months after Europol disrupted it during "Operation Endgame" in May.

Tricky CAPTCHA Caught Dropping Lumma Stealer Malware

darkreading - 22 October 2024 17:10

The persistent infostealer's latest campaign inserts fake CAPTCHA pages into legitimate applications, fooling users into executing the malicious payload, researchers find.

Latrodectus Malware Increasingly Used by Cybercriminals

SecurityWeek - 22 October 2024 11:40

Latrodectus malware has been increasingly used by cybercriminals, with recent campaigns targeting the financial, automotive and healthcare sectors.

Akira ransomware is encrypting victims again following pure extortion fling

The Register - 22 October 2024 16:31

Crooks revert to old ways for greater efficiency Experts believe the Akira ransomware operation is up to its old tricks again, encrypting victims' files after a break from the typical double extortion tactics.

BlackCat Ransomware Successor Cicada3301 Emerges

SecurityWeek - 22 October 2024 12:05

The Cicada3301 ransomware shows multiple similarities with BlackCat and is believed to mark the reemergence of the threat.