Scottish Cyber Coordination Centre

Daily threat bulletin

9 December 2024

Vulnerabilities

U.S. CISA adds CyberPanel flaw to its Known Exploited Vulnerabilities catalog

Security Affairs - 06 December 2024 13:18

U.S. Cybersecurity and Infrastructure Security Agency (CISA) adds CyberPanel flaw to its Known Exploited Vulnerabilities catalog. The U.S. Cybersecurity and Infrastructure Security Agency (CISA) added the CyberPanel flaw CVE-2024-51378 (CVSS score: 10.0) to its Known Exploited Vulnerabilities (KEV) catalog.

New Windows zero-day exposes NTLM credentials, gets unofficial patch

BleepingComputer - 06 December 2024 12:32

A new zero-day vulnerability has been discovered that allows attackers to capture NTLM credentials by simply tricking the target into viewing a malicious file in Windows Explorer. [...]

PoC Exploit Published for Unpatched Mitel MiCollab Vulnerability

SecurityWeek - 06 December 2024 12:31

WatchTowr has published proof-of-concept (PoC) code for an unpatched vulnerability in the Mitel MiCollab enterprise collaboration platform.

SonicWall Patches 6 Vulnerabilities in Secure Access Gateway

SecurityWeek - 06 December 2024 13:26

SonicWall has released patches for multiple high-severity flaws in the SMA100 SSL-VPN secure access gateway.

Exploits and vulnerabilities in Q3 2024

Securelist - 06 December 2024 11:00

The report contains statistics on vulnerabilities and exploits, with an analysis of interesting vulnerabilities found in Q3 2024, such as regreSSHion

Threat actors and malware

Hackers Leveraging Cloudflare Tunnels, DNS Fast-Flux to Hide GammaDrop Malware

The Hacker News - 06 December 2024 13:33

The threat actor known as Gamaredon has been observed leveraging Cloudflare Tunnels as a tactic to conceal its staging infrastructure hosting a malware called GammaDrop.The activity is part of an ongoing spear-phishing campaign targeting Ukrainian entities since at least early

2024 that's designed to drop the Visual Basic Script malware, Recorded Future's Insikt Group said in a new analysis.

Hackers Using Fake Video Conferencing Apps to Steal Web3 Professionals' Data

The Hacker News - 07 December 2024 14:48

Cybersecurity researchers have warned of a new scam campaign that leverages fake video conferencing apps to deliver an information stealer called Realst targeting people working in Web3 under the guise of fake business meetings.

Blue Yonder SaaS giant breached by Termite ransomware gang

BleepingComputer - 06 December 2024 12:35

The Termite ransomware gang has officially claimed responsibility for the November breach of software as a service (SaaS) provider Blue Yonder. [...]

2025 Cyber threat landscape predictions: Emerging data-theft techniques

Security Magazine - 06 December 2024 09:30

At the end of the final quarter, it's essential to reflect on the trends that dominated the cyber threat landscape throughout the year.

UK related

Deloitte Denies Breach, Claims Cyber-Attack Targeted Single Client

Infosecurity Magazine - 06 December 2024 11:54

Despite claims by Brain Cipher that the ransomware gang had targeted Deloitte, the consultancy firm says its systems have not been affected