Scottish
Cyber
Coordination
Centre

Daily threat bulletin

17 January 2025

Vulnerabilities

W3 Total Cache plugin flaw exposes 1 million WordPress sites to attacks

BleepingComputer - 16 January 2025 16:36

A severe flaw in the W3 Total Cache plugin installed on more than one million WordPress sites could give attackers access to various information, including metadata on cloud-based apps. […]

Researchers Find Exploit Allowing NTLMv1 Despite Active Directory Restrictions

The Hacker News - 16 January 2025 17:50

Cybersecurity researchers have found that the Microsoft Active Directory Group Policy that's designed to disable NT LAN Manager (NTLM) v1 can be trivially bypassed by a misconfiguration."A simple misconfiguration in on-premise applications can override the Group Policy, effectively negating the Group Policy designed to stop NTLMv1 authentications," Silverfort researcher Dor Segal said.

Trusted Apps Sneak a Bug Into the UEFI Boot Process

darkreading - 16 January 2025 12:00

Seven system recovery programs contained what amounted to a backdoor for injecting any untrusted file into the system startup process.

Vulnerabilities in SimpleHelp Remote Access Software May Lead to System Compromise

SecurityWeek - 17 January 2025 06:02

Three vulnerabilities in SimpleHelp could allow attackers to compromise the remote access software's server and the client machine.

Millions of Internet Hosts Vulnerable to Attacks Due to Tunneling Protocol Flaws

SecurityWeek - 16 January 2025 14:49

New research shows that over 4 million systems on the internet, including VPN servers and home routers, are vulnerable to attacks due to tunneling protocol flaws.

Threat actors and malware

Clop Ransomware exploits Cleo File Transfer flaw: dozens of claims, disputed breaches

Security Affairs - 16 January 2025 16:36

The Clop ransomware gang claims dozens of victims from a Cleo file transfer vulnerability, though several companies dispute the breaches. The Clop ransomware group added 59 new companies to its leak site, the gain claims to have breached them by exploiting a vulnerability in Cleo file transfer products.

Python-Based Malware Powers RansomHub Ransomware to Exploit Network Flaws

The Hacker News - 16 January 2025 13:15

Cybersecurity researchers have detailed an attack that involved a threat actor utilizing a Python-based backdoor to maintain persistent access to compromised endpoints and then leveraged this access to deploy the RansomHub ransomware throughout the target network.

Russia-linked APT Star Blizzard targets WhatsApp accounts

Security Affairs - 17 January 2025 07:22

The Russian group Star Blizzard targets WhatsApp accounts in a new spear-phishing campaign, shifting tactics to avoid detection. In November 2024, Microsoft researchers observed the Russia-linked APT group Star Blizzard targeting WhatsApp accounts via spear-phishing, shifting tactics to avoid detection.

Hackers Use Image-Based Malware and GenAI to Evade Email Security

Infosecurity Magazine - 16 January 2025 10:01

HP Wolf highlighted novel techniques used by attackers to bypass email protections, including embedding malicious code inside images and utilizing GenAI.

North Korean Hackers Targeting Freelance Software Developers

SecurityWeek - 16 January 2025 13:20

North Korea-linked Lazarus Group is targeting freelance software developers to compromise the supply chain.

Data From 15,000 Fortinet Firewalls Leaked by Hackers

SecurityWeek - 16 January 2025 12:20

Hackers have leaked 15,000 Fortinet firewall configurations, which were apparently obtained as a result of exploitation of CVE-2022–40684.