Scottish
Cyber
Coordination
Centre

Daily threat bulletin

23 January 2025

Vulnerabilities

Critical zero-days impact premium WordPress real estate plugins

BleepingComputer - 22 January 2025 18:59

The RealHome theme and the Easy Real Estate plugins for WordPress are vulnerable to two critical severity flaws that allow unauthenticated users to gain administrative privileges. [...]

Cloudflare CDN flaw leaks user location data, even through secure chat apps

BleepingComputer - 22 January 2025 17:32

A security researcher discovered a flaw in Cloudflare's content delivery network (CDN), which could expose a person's general location by simply sending them an image on platforms like Signal and Discord. [...]

Cisco Fixes Critical Privilege Escalation Flaw in Meeting Management (CVSS 9.9)

The Hacker News - 23 January 2025 12:51

Cisco has released software updates to address a critical security flaw impacting Meeting Management that could permit a remote, authenticated attacker to gain administrator privileges on susceptible instances.

Hackers Exploit Zero-Day in cnPilot Routers to Deploy AIRASHI DDoS Botnet

The Hacker News - 22 January 2025 20:23

Threat actors are exploiting an unspecified zero-day vulnerability in Cambium Networks cnPilot routers to deploy a variant of the AISURU botnet called AIRASHI to carry out distributed denial-of-service (DDoS) attacks.

CISA and FBI Release Advisory on How Threat Actors Chained Vulnerabilities in Ivanti Cloud Service Applications

CISA Advisories -

CISA, in partnership with the Federal Bureau of Investigation (FBI), released Threat Actors Chained Vulnerabilities in Ivanti Cloud Service Applications. This advisory was crafted in response to active exploitation of vulnerabilities—CVE-2024-8963, an administrative bypass vulnerability; CVE-2024-9379, a SQL injection vulnerability; and CVE-2024-8190 and CVE-2024-9380, remote code execution vulnerabilities—in Ivanti Cloud Service Appliances (CSA) in September 2024.

Threat actors and malware

PlushDaemon APT Targets South Korean VPN Provider in Supply Chain Attack

The Hacker News - 22 January 2025 15:19

A previously undocumented China-aligned advanced persistent threat (APT) group named PlushDaemon has been linked to a supply chain attack targeting a South Korean virtual private network (VPN) provider in 2023, according to new findings from ESET.

Supply chain attack hits Chrome extensions, could expose millions

The Register - 22 January 2025 20:45

Threat actor exploited phishing and OAuth abuse to inject malicious code Cybersecurity outfit Sekoia is warning Chrome users of a supply chain attack targeting browser extension developers that has potentially impacted hundreds of thousands of individuals already.

Hackers exploit 16 zero-days on first day of Pwn2Own Automotive 2025

BleepingComputer - 22 January 2025 10:38

On the first day of Pwn2Own Automotive 2025, security researchers exploited 16 unique zero-days and collected $382,750 in cash awards. [...]

Cyber Insights 2025: APIs – The Threat Continues

SecurityWeek - 22 January 2025 15:00

APIs are easy to develop, simple to implement, and frequently attacked. They are prime and lucrative targets for cybercriminals.

UK related

UK Mail Check: DMARC Reporting Changes to Know

Security Boulevard - 22 January 2025 21:51

The UK National Cyber Security Centre (NCSC), the country’s technical authority for cyber security, has announced changes to its Mail Check program.

73% of UK Education Sector Hit by Cyber-Attacks in Past Five Years

Infosecurity Magazine - 22 January 2025 15:10

New ESET research reveals that 73% of UK educational institutions experienced at least one cyber-attack or breach in the past five years