Scottish Cyber Coordination Centre

Daily Threat Bulletin

06 November 2025

Vulnerabilities

CISA warns of critical CentOS Web Panel bug exploited in attacks

BleepingComputer - 05 November 2025 14:26

The U.S. Cybersecurity & Infrastructure Security Agency (CISA) is warning that threat actors are exploiting a critical remote command execution flaw in CentOS Web Panel (CWP).

Critical Site Takeover Flaw Affects 400K WordPress Sites

darkreading - 05 November 2025 15:35

Attackers are already targeting a vulnerability in the Post SMTP plug-in that allows them to fully compromise an account and website for nefarious purposes.

AMD red-faced over random-number bug that kills cryptographic security

The Register - 05 November 2025 16:01

Local privileges required to exploit flaw in Ryzen and Epyc CPUs. Some patches available, more on the way AMD will issue a microcode patch for a high-severity vulnerability that could weaken cryptographic keys across Epyc and Ryzen CPUs.

Researchers Find ChatGPT Vulnerabilities That Let Attackers Trick AI Into Leaking Data

The Hacker News - 05 November 2025 20:34

Cybersecurity researchers have disclosed a new set of vulnerabilities impacting OpenAI's ChatGPT artificial intelligence (AI) chatbot that could be exploited by an attacker to steal personal information from users' memories and chat histories without their knowledge.

Threat actors and malware

Gootloader malware is back with new tricks after 7-month break

BleepingComputer - 05 November 2025 17:52

The Gootloader malware loader operation has returned after a 7-month absence and is once again performing SEO poisoning to promote fake websites that distribute the malware.

Hackers Weaponize Windows Hyper-V to Hide Linux VM and Evade EDR Detection

The Hacker News - 06 November 2025 13:52

The threat actor known as Curly COMrades has been observed exploiting virtualization technologies as a way to bypass security solutions and execute custom malware.

Scottish Cyber Coordination Centre

SonicWall Confirms State-Sponsored Hackers Behind September Cloud Backup Breach

The Hacker News - 06 November 2025 12:10

SonicWall has formally implicated state-sponsored threat actors as behind the September security breach that led to the unauthorized exposure of firewall configuration backup files.

Google Uncovers PROMPTFLUX Malware That Uses Gemini AI to Rewrite Its Code Hourly

The Hacker News - 05 November 2025 22:03

Google on Wednesday said it discovered an unknown threat actor using an experimental Visual Basic Script (VB Script) malware dubbed PROMPTFLUX that interacts with its Gemini artificial intelligence (AI) model API to write its own source code for improved obfuscation and evasion.

Malware Now Uses AI During Execution to Mutate and Collect Data, Google Warns

SecurityWeek - 05 November 2025 16:25

Google has released a report describing the novel ways in which malware has been using AI to adapt and evade detection.The post Malware Now Uses AI During Execution to Mutate and Collect Data, Google Warns appeared first on SecurityWeek.

Nikkei Says 17,000 Impacted by Data Breach Stemming From Slack Account Hack

SecurityWeek - 05 November 2025 12:24

The Japanese media giant says compromised Slack credentials were used to steal employee and business partner information. The post Nikkei Says 17,000 Impacted by Data Breach Stemming From Slack Account Hack appeared first on SecurityWeek.

UNK_SmudgedSerpent Targets Academics With Political Lures

Infosecurity Magazine - 05 November 2025 17:00

A previously unknown cyber actor UNK_SmudgedSerpent has been observed targeting academics with phishing and malware, merging techniques from Iranian groups.

Hundreds of Malware-Laden Apps Downloaded 42 Million Times From Google Play

Infosecurity Magazine - 05 November 2025 10:30

Zscaler estimates 239 malicious Android apps made it onto the official Play store over the past year

UK related

UK carriers to block spoofed phone numbers in fraud crackdown

BleepingComputer - 05 November 2025 12:33

Scottish Cyber Coordination Centre

Under a new partnership with the government aimed at combating fraud, Britain's largest mobile carriers have committed to upgrading their networks to eliminate scammers' ability to spoof phone numbers within a year.

M&S pegs cyberattack cleanup costs at £136M as profits slump

The Register - 05 November 2025 12:54

Retailer's tech systems aren't down anymore, but the same can't be said for its rocky financials Marks & Spencer says its April cyberattack will cost around £136 million ($177.2 million) in total.

UK agri dept spent hundreds of millions upgrading to Windows 10 – just in time for end of support

The Register - 05 November 2025 10:21

After a £312M upgrade to the retiring OS, Defra still has 24,000 devices to replace The UK's Department for Environment, Food & Rural Affairs (Defra) has spent £312 million (c $407 million) modernizing its IT estate, including replacing tens of thousands of Windows 7 laptops with Windows 10 – which officially reached end of support last month.