Scottish Cyber Coordination Centre

Daily Threat Bulletin

17 April 2025

Vulnerabilities

CISA Adds One Known Exploited Vulnerability to Catalog

CISA Advisories -

CISA has added one new vulnerability to its Known Exploited Vulnerabilities Catalog, based on evidence of active exploitation.

CVE-2021-20035 - SonicWall SMA100 Appliances OS Command Injection Vulnerability.

Apple fixes two zero-days exploited in targeted iPhone attacks

BleepingComputer - 16 April 2025 15:06

Apple released emergency security updates to patch two zero-day vulnerabilities that were used in an “extremely sophisticated attack” against specific targets’ iPhones.

New Windows Task Scheduler Bugs Let Attackers Bypass UAC and Tamper with Logs

The Hacker News - 16 April 2025 22:48

Cybersecurity researchers have detailed four different vulnerabilities in a core component of the Windows task scheduling service that could be exploited by local attackers to achieve privilege escalation and erase logs to cover up evidence of malicious activities.

Chrome 135, Firefox 137 Updates Patch Severe Vulnerabilities

SecurityWeek - 16 April 2025 11:35

Chrome 135 and Firefox 137 updates have been rolled out with patches for critical- and high-severity vulnerabilities.

Patch Now: NVDIA Flaws Expose AI Models, Critical Infrastructure

darkreading - 16 April 2025 17:33

A fix for a critical flaw in a tool allowing organizations to run GPU-accelerated containers released last year did not fully mitigate the issue, spurring the need to patch a secondary flaw to protect organizations that rely on NVIDIA processors for AI workloads.

MITRE CVE Program Uncertainty: In last-minute reversal, US agency extends support for cyber vulnerability database

Reuters - 16 April 2025 10:41

U.S. officials will extend support for 11 months for a database of cyber weaknesses that plays a critical role in fighting bugs and hacks, a spokesperson said on Wednesday, just as the funding was due to run out.

Scottish Cyber Coordination Centre

Threat actors and malware

China-Backed Hackers Exploit BRICKSTORM Backdoor to Spy on European Businesses

Infosecurity Magazine - 16 April 2025 15:00

NVISO discovered new variants of the BRICKSTORM backdoor, initially designed for Linux, on Windows systems

Microsoft Warns of Node.js Abuse for Malware Delivery

SecurityWeek - 16 April 2025 12:00

In the past months Microsoft has seen multiple campaigns involving Node.js to deliver malware and other malicious payloads.

CISA warns of potential data breaches caused by legacy Oracle Cloud leak

The Record from Recorded Future News - 16 April 2025 21:35

Federal cybersecurity officials on Wednesday warned of the potential fallout of a data breach impacting Oracle.

The Sophos Annual Threat Report: Cybercrime on Main Street 2025

Threat Research – Sophos News - 16 April 2025 11:00

Ransomware remains the biggest threat, but old and misconfigured network devices are making it too easy

Cyber Threats Against Energy Sector Surge as Global Tensions Mount

Security Affairs - 16 April 2025 09:27

Resecurity warns about the increase in targeted cyberattacks against enterprises in the energy sector worldwide. Some of these attacks represent much larger campaigns designed to target country-level infrastructure, acting as tools for geopolitical influence.

UK incidents

British law firm fined after ransomware group publishes confidential client data

The Record from Recorded Future News - 16 April 2025 13:41

A British law firm has been fined £60,000 ($80,000) after cybercriminals accessed the company's case management system and published sensitive information on the dark web, something the company only learned about after being contacted by the National Crime Agency.