Scottish
Cyber
Coordination
Centre

Daily Threat Bulletin

28 January 2025

Vulnerabilities

Apple fixes this year’s first actively exploited zero-day bug

BleepingComputer - 27 January 2025 15:17

Apple has released security updates to fix this year's first zero-day vulnerability, tagged as actively exploited in attacks targeting iPhone users.

Multiple Git flaws led to credentials compromise

Security Affairs - 27 January 2025 15:35

Security researcher RyotaK from GMO Flatt Security Inc discovered multiple vulnerabilities in the Git credential retrieval protocol that could have allowed threat actors to access user credentials.

Threat actors and malware

DeepSeek halts new signups amid "large-scale" cyberattack

BleepingComputer - 27 January 2025 18:01

Chinese AI platform DeepSeek has disabled registrations on it DeepSeek-V3 chat platform due to an ongoing "large-scale" cyberattack targeting its services.

ESXi ransomware attacks use SSH tunnels to avoid detection

Security Affairs - 27 January 2025 11:05

Researchers at cybersecurity firm Sygnia warn that threat actors behind ESXi ransomware attacks target virtualized environments using SSH tunneling to avoid detection.

GamaCopy Mimics Gamaredon Tactics in Cyber Espionage Targeting Russian Entities

The Hacker News - 27 January 2025 14:29

A previously unknown threat actor has been observed copying the tradecraft associated with the Kremlin-aligned Gamaredon hacking group in its cyber attacks targeting Russian-speaking entities.The campaign has been attributed to a threat cluster dubbed GamaCopy, which is assessed to share overlaps with another hacking group named Core Werewolf, also tracked as Awaken Likho and PseudoGamaredon.

Bitwarden makes it harder to hack password vaults without MFA

BleepingComputer - 27 January 2025 17:00

Open-source password manager Bitwarden is adding an extra layer of security for accounts that are not protected by two-factor authentication, requiring email verification before allowing access to accounts.

UK Related

British Museum says ex-contractor 'shut down' IT systems, wreaked havoc

The Register - 27 January 2025 10:30

Former freelancer cuffed a week after being dismissed by UK's top visitor attraction The British Museum was forced to temporarily close some galleries and exhibitions this weekend after a disgruntled former tech contractor went rogue and shuttered some onsite IT systems.

TalkTalk confirms data breach involving a third-party platform

Security Affairs - 27 January 2025 21:00

UK telecommunications company TalkTalk confirmed a data breach after a threat actor claimed responsibility for the cyber attack on a cybercrime forum and offered for sale alleged customer data.