Scottish
Cyber
Coordination
Centre

Daily threat bulletin

21 October 2024

Vulnerabilities

Severe flaws in E2EE cloud storage platforms used by millions

BleepingComputer - 20 October 2024 13:06

Several end-to-end encrypted (E2EE) cloud storage platforms are vulnerable to a set of security issues that could expose user data to malicious actors. [...]

MacOS Safari 'HM Surf' Exploit Exposes Camera, Mic, Browser Data

darkreading - 18 October 2024 22:26

Microsoft researchers toyed with app permissions to uncover CVE-2024-44133, using it to access sensitive user data.

Hackers Exploit Roundcube Webmail XSS Vulnerability to Steal Login Credentials

The Hacker News - 20 October 2024 14:07

Unknown threat actors have been observed attempting to exploit a now-patched security flaw in the open-source Roundcube webmail software as part of a phishing attack designed to steal user credentials.

U.S. CISA adds Veeam Backup and Replication flaw to its Known Exploited Vulnerabilities catalog

Security Affairs - 19 October 2024 16:22

U.S. Cybersecurity and Infrastructure Security Agency (CISA) adds Veeam Backup and Replication vulnerability to its Known Exploited Vulnerabilities catalog. The U.S. Cybersecurity and Infrastructure Security Agency (CISA) added the Veeam Backup and Replication flaw CVE-2024-40711 (CVSS score of 9.8).

Open source LLM tool primed to sniff out Python zero-days

The Register - 20 October 2024 10:00

The static analyzer uses Claude AI to identify vulns and suggest exploit code Researchers with Seattle-based Protect AI plan to release a free, open source tool that can find zero-day vulnerabilities in Python codebases with the help of Anthropic's Claude AI model....

Threat actors and malware

Cisco takes DevHub portal offline after hacker publishes stolen data

BleepingComputer - 18 October 2024 19:21

Cisco confirmed today that it took its public DevHub portal offline after a threat actor leaked “non-public” data, but it continues to state that there is no evidence that its systems were breached. [...]

North Korea-linked APT37 exploited IE zero-day in a recent attack

Security Affairs - 19 October 2024 15:07

North Korea-linked group APT37 exploited an Internet Explorer zero-day vulnerability in a supply chain attack. A North Korea-linked threat actor, tracked as APT37 (also known as RedEyes, TA-RedAnt, Reaper, ScarCruft, Group123), exploited a recent Internet Explorer zero-day vulnerability, tracked as CVE-2024-38178 (CVSS score 7.5), in a supply chain attack.

North Korean IT Workers in Western Firms Now Demanding Ransom for Stolen Data

The Hacker News - 20 October 2024 13:53

North Korean information technology (IT) workers who obtain employment under false identities in Western companies are not only stealing intellectual property, but are also stepping up by demanding ransoms in order to not leak it, marking a new twist to their financially motivated attacks.