Scottish Cyber Coordination Centre

Daily threat bulletin

17 July 2024

Vulnerabilities

CISA warns critical Geoserver GeoTools RCE flaw is exploited in attacks

BleepingComputer - 16 July 2024 19:14

CISA is warning that a critical GeoServer GeoTools remote code execution flaw tracked as CVE-2024-36401 is being actively exploited in attacks. [...]

Microsoft finally fixes Outlook alerts bug caused by December updates

BleepingComputer - 16 July 2024 09:17

Microsoft has finally fixed a known Outlook issue, confirmed in February, which was triggering incorrect security alerts after installing the December security updates for Outlook Desktop. [...]

Critical Apache HugeGraph Vulnerability Under Attack - Patch ASAP

The Hacker News - 17 July 2024 11:55

Threat actors are actively exploiting a recently disclosed critical security flaw impacting Apache HugeGraph-Server that could lead to remote code execution attacks.Tracked as CVE-2024-27348 (CVSS score: 9.8), the vulnerability impacts all versions of the software before 1.3.0. It has been described as a remote command execution flaw in the Gremlin graph traversal language API.

Threat actors and malware

Scattered Spider Adopts RansomHub and Qilin Ransomware for Cyber Attacks

The Hacker News - 17 July 2024 12:20

The infamous cybercrime group known as Scattered Spider has incorporated ransomware strains such as RansomHub and Qilin into its arsenal, Microsoft has revealed.

Iranian Hackers Deploy New BugSleep Backdoor in Middle East Cyber Attacks

The Hacker News - 16 July 2024 15:43

The Iranian nation-state actor known as MuddyWater has been observed using a never-before-seen backdoor as part of a recent attack campaign, shifting away from its well-known tactic of deploying legitimate remote monitoring and management (RMM) software for maintaining persistent access.

Snowflake Account Attacks Driven by Exposed Legitimate Credentials

darkreading - 17 July 2024 15:00

Scottish Cyber Coordination Centre

Credential management gets a boost with the latest infostealers' extortion campaign built on info stolen from cloud storage systems.

Void Banshee APT Exploits Microsoft Zero-Day in Spear-Phishing Attacks

darkreading - 16 July 2024 15:30

The threat group used CVE-2024-38112 and a "zombie" version of IE to spread Atlantida Stealer through purported PDF versions of reference books.

Hackers Exploit Flaw in Squarespace Migration to Hijack Domains

SecurityWeek - 16 July 2024 12:03

Hackers exploited a flaw to hijack cryptocurrency domains that were migrated from Google Domains to Squarespace. The post Hackers Exploit Flaw in Squarespace Migration to Hijack Domains appeared first on SecurityWeek.

UK incidents

Privacy warriors gripe to UK watchdog about Meta harvesting user data to train AI

The Register - 16 July 2024 12:25

Move follows Instagram and Facebook giant's decision to reverse direction in EU after protests A UK data rights campaign group has launched a complaint with the data law regulator against Meta's change of privacy policy which allows it to scrape user data to develop AI models.