Scottish
Cyber
Coordination
Centre

Daily Threat Bulletin

02 December 2024

Vulnerabilities

Zabbix urges upgrades after critical SQL injection bug disclosure

The Register - 29 November 2024 18:44

US agencies blasted 'unforgivable' SQLi flaws earlier this year Open-source enterprise network and application monitoring provider Zabbix is warning customers of a new critical vulnerability that could lead to full system compromise.

Microsoft Fixes AI, Cloud, and ERP Security Flaws; One Exploited in Active Attacks

The Hacker News - 29 November 2024 16:04

Microsoft has addressed four security flaws impacting its artificial intelligence (AI), cloud, enterprise resource planning, and Partner Center offerings, including one that it said has been exploited in the wild. The vulnerability that has been tagged with an "Exploitation Detected" assessment is CVE-2024-49035 (CVSS score: 8.7).

New Windows Server 2012 zero-day gets free, unofficial patches

BleepingComputer - 29 November 2024 13:00

Free unofficial security patches have been released through the 0patch platform to address a zero-day vulnerability introduced over two years ago in the Windows Mark of the Web (MotW) security mechanism.

Threat actors and malware

SpyLoan Android malware on Google play installed 8 million times

BleepingComputer - 30 November 2024 11:11

A new set of 15 SpyLoan Android malware apps with over 8 million installs was discovered on Google Play, targeting primarily users from South America, Southeast Asia, and Africa.

New Rockstar 2FA phishing service targets Microsoft 365 accounts

BleepingComputer - 29 November 2024 15:01

A new phishing-as-a-service (PhaaS) platform named 'Rockstar 2FA' has emerged, facilitating large-scale adversary-in-the-middle (AiTM) attacks to steal Microsoft 365 credentials.

IT threat evolution Q3 2024

Securelist - 29 November 2024 11:00

In this part of the malware report we discuss the most remarkable findings of Q3 2024, including APT and hacktivist attacks, ransomware, stealers, macOS malware and so on.

Wanted Russian Hacker Linked to Hive and LockBit Ransomware Arrested

The Hacker News - 30 November 2024 13:44

A Russian cybercriminal wanted in the U.S. in connection with LockBit and Hive ransomware operations has been arrested by law enforcement authorities in the country.

UK incidents

INC Ransom Claims Cyber-Attack on UK Children's Hospital

Infosecurity Magazine - 29 November 2024 12:50

The infamous ransomware group has claimed to have compromised sensitive data from a children's hospital in Liverpool, UK. The NHS Trust is investigating the incident with the help of the National Crime Agency.