Scottish
Cyber
Coordination
Centre

Daily threat bulletin

18 November 2024

Vulnerabilities

Security plugin flaw in millions of WordPress sites gives admin access

BleepingComputer - 17 November 2024 11:19

A critical authentication bypass vulnerability has been discovered impacting the WordPress plugin 'Really Simple Security' (formerly 'Really Simple SSL'), including both free and Pro versions. [...]

NSO Group Exploited WhatsApp to Install Pegasus Spyware Even After Meta's Lawsuit

The Hacker News - 18 November 2024 12:22

Legal documents released as part of an ongoing legal tussle between Meta's WhatsApp and NSO Group have revealed that the Israeli spyware vendor used multiple exploits targeting the messaging app to deliver Pegasus, including one even after it was sued by Meta for doing so.

High-Severity Flaw in PostgreSQL Allows Hackers to Exploit Environment Variables

The Hacker News - 15 November 2024 13:10

Cybersecurity researchers have disclosed a high-severity security flaw in the PostgreSQL open-source database system that could allow unprivileged users to alter environment variables, and potentially lead to code execution or information disclosure.The vulnerability, tracked as CVE-2024-10979, carries a CVSS score of 8.8.

Warning: DEEPDATA Malware Exploiting Unpatched Fortinet Flaw to Steal VPN Credentials

The Hacker News - 16 November 2024 12:55

A threat actor known as BrazenBamboo has exploited an unresolved security flaw in Fortinet's FortiClient for Windows to extract VPN credentials as part of a modular framework called DEEPDATA.Volexity, which disclosed the findings Friday, said it identified the zero-day exploitation of the credential disclosure vulnerability in July 2024.

Palo Alto updates advisory about firewall bug after discovering exploitation attempts

The Record from Recorded Future News - 15 November 2024 19:55

Threat actors and malware

Botnet exploits GeoVision zero-day to install Mirai malware

BleepingComputer - 15 November 2024 15:39

A malware botnet is exploiting a zero-day vulnerability in end-of-life GeoVision devices to compromise and recruit them for likely DDoS or cryptomining attacks. [...]

Glove Stealer Malware Bypasses Chrome’s App-Bound Encryption

SecurityWeek - 15 November 2024 14:24

The Glove Stealer malware leverages a recently disclosed App-Bound encryption bypass method in attacks.

Iranian Hackers Deploy WezRat Malware in Attacks Targeting Israeli Organizations

The Hacker News - 16 November 2024 00:27

Cybersecurity researchers have shed light on a new remote access trojan and information stealer used by Iranian state-sponsored actors to conduct reconnaissance of compromised endpoints and execute malicious commands.

GitHub projects targeted with malicious commits to frame researcher

BleepingComputer - 16 November 2024 11:30

GitHub projects have been targeted with malicious commits and pull requests, in an attempt to inject backdoors into these projects.

Ransomware Groups Use Cloud Services For Data Exfiltration

Infosecurity Magazine - 15 November 2024 11:00

SentinelOne described some of ransomware groups’ favorite techniques for targeting cloud services.