Scottish Cyber Coordination Centre

Daily threat bulletin

28 August 2024

Vulnerabilities

Critical flaw in WPML WordPress plugin impacts 1M websites

Security Affairs - 27 August 2024 22:38

A critical flaw in the WPML WordPress plugin, which is installed on 1 million websites, could allow potential compromise of affected sites. The WPML Multilingual CMS Plugin for WordPress is installed on over 1 million sites.

Chinese Volt Typhoon hackers exploited Versa zero-day to breach ISPs, MSPs

BleepingComputer - 27 August 2024 11:00

The Chinese state-backed hacking group Volt Typhoon is behind attacks that exploited a zero-day flaw in Versa Director to upload a custom webshell to steal credentials and breach corporate networks.

CISA Flags Critical Apache OFBiz Flaw Amid Active Exploitation Reports

The Hacker News - 28 August 2024 11:35

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) on Tuesday added a critical security flaw affecting the Apache OFBiz open-source enterprise resource planning (ERP) system to its Known Exploited Vulnerabilities (KEV) catalog, citing evidence of active exploitation in the wild.

PoC Exploit for Zero-Click Vulnerability Made Available to the Masses

darkreading - 27 August 2024 21:56

The exploit can be accessed on GitHub and makes it easier for the flaw to be exploited by threat actors.

Threat actors and malware

Microsoft's Sway Serves as Launchpad for 'Quishing' Campaign

darkreading - 27 August 2024 20:05

The attack is a mashup of QR codes and phishing that gets users to click on links to malicious Web pages.

Threat Group 'Bling Libra' Pivots to Extortion for Cloud Attacks

darkreading - 27 August 2024 12:39

Scottish Cyber Coordination Centre

The ShinyHunters attackers are skipping selling stolen data on hacker forums in favor of using deadline-driven ransom notes for financial gain.

Malware infiltrates Pidgin messenger's official plugin repository

BleepingComputer - 27 August 2024 14:25

The Pidgin messaging app removed the ScreenShareOTR plugin from its official third-party plugin list after it was discovered that it was used to install keyloggers, information stealers, and malware commonly used to gain initial access to corporate networks.