Scottish Cyber Coordination Centre

Daily Threat Bulletin

27 October 2025

Vulnerabilities

Hackers launch mass attacks exploiting outdated WordPress plugins

BleepingComputer - 24 October 2025 16:28

A widespread exploitation campaign is targeting WordPress websites with GutenKit and Hunk Companion plugins vulnerable to critical-severity, old security issues that can be used to achieve remote code execution (RCE). [...]

Critical WSUS flaw in Windows Server now exploited in attacks

BleepingComputer - 24 October 2025 13:28

Attackers are now exploiting a critical-severity Windows Server Update Service (WSUS) vulnerability, which already has publicly available proof-of-concept exploit code. [...]

U.S. CISA adds Microsoft WSUS, and Adobe Commerce and Magento Open Source flaws to its Known Exploited Vulnerabilities catalog

Security Affairs - 24 October 2025 20:05

U.S. Cybersecurity and Infrastructure Security Agency (CISA) adds Microsoft WSUS, and Adobe Commerce and Magento Open Source flaws to its Known Exploited Vulnerabilities catalog. The U.S. Cybersecurity and Infrastructure Security Agency (CISA) added Microsoft WSUS, and Adobe Commerce and Magento Open Source flaws to its Known Exploited Vulnerabilities (KEV) catalog.

OpenAI Atlas Omnibox Is Vulnerable to Jailbreaks

SecurityWeek - 25 October 2025 12:35

Researchers have discovered that a prompt can be disguised as an url, and accepted by Atlas as an url in the omnibox.

Threat actors and malware

New CoPhish attack steals OAuth tokens via Copilot Studio agents

BleepingComputer - 25 October 2025 13:16

A new phishing technique dubbed 'CoPhish' weaponizes Microsoft Copilot Studio agents to deliver fraudulent OAuth consent requests via legitimate and trusted Microsoft domains. [...]

Russian Rosselkhoznadzor hit by DDoS attack, food shipments across Russia delayed

Scottish Cyber Coordination Centre

Security Affairs - 25 October 2025 18:52

A DDoS attack on Russia's food safety agency Rosselkhoznadzor disrupted food shipments by crippling its VetIS and Saturn tracking systems. A DDoS cyberattack on Russia's food safety agency, Rosselkhoznadzor, disrupted nationwide food shipments by knocking offline its VetIS and Saturn tracking systems for agricultural products and chemicals.

China-linked hackers exploit patched ToolShell flaw to breach Middle East telecom

Security Affairs - 24 October 2025 09:37

China-based threat actors exploited ToolShell SharePoint flaw CVE-2025-53770 soon after its July patch. China-linked threat actors exploited the ToolShell SharePoint flaw vulnerability, tracked as CVE-2025-53770, to breach a telecommunications company in the Middle East after it was addressed by Microsoft in July 2025.

APT36 Targets Indian Government with Golang-Based DeskRAT Malware Campaign

The Hacker News - 24 October 2025 20:30

A Pakistan-nexus threat actor has been observed targeting Indian government entities as part of spear-phishing attacks designed to deliver a Golang-based malware known as DeskRAT.The activity, observed in August and September 2025 by Sekoia, has been attributed to Transparent Tribe (aka APT36), a state-sponsored hacking group known to be active since at least 2013.

Self-Spreading 'GlassWorm' Infects VS Code Extensions in Widespread Supply Chain Attack

The Hacker News - 24 October 2025 13:30

Cybersecurity researchers have discovered a self-propagating worm that spreads via Visual Studio Code (VS Code) extensions on the Open VSX Registry and the Microsoft Extension Marketplace, underscoring how developers have become a prime target for attacks.