Scottish Cyber Coordination Centre

Daily threat bulletin

6 January 2025

Vulnerabilities

LDAPNightmare, a PoC exploit targets Windows LDAP flaw CVE-2024-49113

Security Affairs - 03 January 2025 10:42

Experts warn of a new PoC exploit, LDAPNightmare, that targets a Windows LDAP flaw (CVE-2024-49113), causing crashes & reboots. The vulnerability CVE-2024-49113 (CVSS score of 7.5), named LDAPNightmare, is a Windows Lightweight Directory Access Protocol (LDAP) Denial of Service flaw that was discovered by the researcher Yuki Chen. An attacker can exploit the now-patched vulnerability to [...]

Nuclei flaw lets malicious templates bypass signature verification

BleepingComputer - 04 January 2025 18:59

A now-fixed vulnerability in the open-source vulnerability scanner Nuclei could potentially allow attackers to bypass signature verification while sneaking malicious code into templates that execute on local systems. [...]

Severe Security Flaws Patched in Microsoft Dynamics 365 and Power Apps Web API

The Hacker News - 02 January 2025 19:23

Details have emerged about three now-patched security vulnerabilities in Dynamics 365 and Power Apps Web API that could result in data exposure.The flaws, discovered by Melbourne-based cybersecurity company Stratus Security, have been addressed as of May 2024. Two of the three shortcomings reside in Power Platform's OData Web API Filter, while the third vulnerability is rooted in the FetchXML

New "DoubleClickjacking" Exploit Bypasses Clickjacking Protections on Major Websites

The Hacker News - 01 January 2025 19:54

Threat hunters have disclosed a new "widespread timing-based vulnerability class" that leverages a double-click sequence to facilitate clickjacking attacks and account takeovers in almost all major websites.

CISA Adds One Known Exploited Vulnerability to Catalog

CISA Advisories -

CISA has added one new vulnerability to its Known Exploited Vulnerabilities Catalog, based on evidence of active exploitation - CVE-2024-3393 Palo Alto Networks PAN-OS Malformed DNS Packet Vulnerability.

Scottish Cyber Coordination Centre

Threat actors and malware

New FireScam Android data-theft malware poses as Telegram Premium app

BleepingComputer - 04 January 2025 11:16

A new Android malware named 'FireScam' is being distributed as a premium version of the Telegram app via phishing websites on GitHub that mimick the RuStore, Russia's app market for mobile devices. [...]

Global Campaign Targets PlugX Malware with Innovative Portal

Infosecurity Magazine - 02 January 2025 18:15

Sekoia's innovative PlugX malware disinfection campaign removed active threats across ten countries

Hackers target dozens of VPN and AI extensions for Google Chrome to compromise data

The Record from Recorded Future News - 02 January 2025 20:56

US Treasury Department sanctioned Chinese cybersecurity firm linked to Flax Typhoon APT

Security Affairs - 04 January 2025 20:26

The U.S. Treasury Department sanctioned Chinese cybersecurity firm Integrity Tech for its involvement in attacks attributed to the Flax Typhoon group. The U.S. Treasury sanctioned a Chinese cybersecurity firm, Integrity Tech, for links to cyberattacks by China's state-backed Flax Typhoon APT group (also called Ethereal Panda or RedJuliett).

Chinese APT Exploits BeyondTrust API Key to Access U.S. Treasury Systems and Documents

The Hacker News - 31 December 2024 12:12

The United States Treasury Department said it suffered a "major cybersecurity incident" that allowed suspected Chinese threat actors to remotely access some computers and unclassified documents. "On December 8, 2024, Treasury was notified by a third-party software service provider, BeyondTrust, that a threat actor had gained access to a key used by the vendor to secure a cloud-based

In Other News: Volkswagen Data Leak, DoubleClickjacking, China Denies Hacking US Treasury

SecurityWeek - 03 January 2025 13:59

Noteworthy stories that might have slipped under the radar: location data of 800,000 electric Volkswagen cars leaked, DoubleClickjacking attack, China denies hacking US Treasury.