Scottish
Cyber
Coordination
Centre

Daily Threat Bulletin

19 August 2024

Vulnerabilities

CISA adds SolarWinds Web Help Desk bug to its Known Exploited Vulnerabilities catalog

Security Affairs - 16 August 2024 21:13

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) added SolarWinds Web Help Desk deserialization of untrusted data vulnerability, tracked as CVE-2024-28986 (CVSS score of 9.8), to its Known Exploited Vulnerabilities (KEV) catalog.

Copy2Pwn Zero-Day Exploited to Bypass Windows Protections

SecurityWeek - 16 August 2024 09:45

ZDI details a zero-day named Copy2Pwn and tracked as CVE-2024-38213, which cybercriminals exploited to bypass MotW protections in Windows.

Threat actors and malware

Azure domains and Google abused to spread disinformation and malware

BleepingComputer - 17 August 2024 10:00

A clever disinformation campaign engages several Microsoft Azure and OVH cloud subdomains as well as Google search to promote malware and spam sites.

The Mad Liberator ransomware group uses social-engineering techniques

Security Affairs - 19 August 2024 01:00

New cybercrime group Mad Liberator is targeting AnyDesk users and runs a fake Microsoft Windows update screen to conceal data exfiltrating. The Sophos X-Ops Incident Response team warned that a new ransomware group called Mad Liberator is exploiting the remote-access application Anydesk for their attacks.

Large-scale extortion campaign targets publicly accessible environment variable files (.env)

Security Affairs - 18 August 2024 08:17

A large-scale extortion campaign compromised multiple organizations by exploiting publicly accessible environment variable files (.env). Palo Alto Unit 42 researchers uncovered a large-scale extortion campaign that successfully compromised and extorted multiple victim organizations by leveraging exposed environment variable files (.env files).

OpenAI Blocks Iranian Influence Operation Using ChatGPT for U.S. Election Propaganda

The Hacker News - 17 August 2024 13:08

OpenAI on Friday said it banned a set of accounts linked to what it said was an Iranian covert influence operation that leveraged ChatGPT to generate content that, among other things, focused on the upcoming U.S. presidential election.

New Banshee Stealer Targets 100+ Browser Extensions on Apple macOS Systems

The Hacker News - 16 August 2024 14:58

Cybersecurity researchers have uncovered new stealer malware that's designed to specifically target Apple macOS systems. Dubbed Banshee Stealer, it's offered for sale in the cybercrime underground for a steep price of $3,000 a month and works across both x86_64 and ARM64 architectures.

RansomHub-linked EDR-killing malware spotted in the wild

The Register - 19 August 2024 02:52

Malware that kills endpoint detection and response (EDR) software has been spotted on the scene and, given it's deploying RansomHub, it could soon be prolific.