Scottish
Cyber
Coordination
Centre

Daily Threat Bulletin

14 April 2025

Vulnerabilities

Fortinet Warns Attackers Retain FortiGate Access Post-Patching via SSL-VPN Symlink Exploit

The Hacker News - 12 April 2025 00:25

Fortinet has revealed that threat actors have found a way to maintain read-only access to vulnerable FortiGate devices even after the initial access vector used to breach the devices was patched.The attackers are believed to have leveraged known and now-patched security flaws, including, but not limited to, CVE-2022-42475, CVE-2023-27997, and CVE-2024-21762.

10 Bugs Found in Perplexity AI's Chatbot Android App

darkreading - 11 April 2025 14:00

Researchers characterize the company's artificial intelligence chatbot as less secure than ChatGPT and even DeepSeek.

Vulnerability in OttoKit WordPress Plugin Exploited in the Wild

SecurityWeek - 11 April 2025 13:15

A vulnerability in the OttoKit WordPress plugin with over 100,000 active installations has been exploited in the wild.

SonicWall Patches High-Severity Vulnerability in NetExtender

SecurityWeek - 11 April 2025 12:00

SonicWall has released fixes for three vulnerabilities in NetExtender for Windows, including a high-severity bug.

NVD Revamps Operations as Vulnerability Reporting Surges

Infosecurity Magazine - 11 April 2025 16:05

The NVD program manager has announced undergoing process improvements to catch up with its growing vulnerability backlog

Cyble Urges Critical Vulnerability Fixes Affecting Industrial Systems

Infosecurity Magazine - 11 April 2025 09:00

Rockwell Automation, Hitachi Energy and Inaba Denki Sangyo have products affected by critical vulnerabilities carrying severity ratings as high as 9.9

Exploit Attempts for Recent Langflow AI Vulnerability (CVE-2025-3248), (Sat, Apr 12th)

SANS Internet Storm Centre - 13 April 2025 01:21

Two weeks ago, version 1.3.0 of Langflow was released. The release notes list many fixes but do not mention that one of the “Bug Fixes” addresses a major vulnerability. Instead, the release notes state, “auth current user on code validation.” [1]

Threat actors and malware

Tycoon2FA phishing kit targets Microsoft 365 with new tricks

BleepingComputer - 12 April 2025 12:16

Phishing-as-a-service (PhaaS) platform Tycoon2FA, known for bypassing multi-factor authentication on Microsoft 365 and Gmail accounts, has received updates that improve its stealth and evasion capabilities. [...]

Microsoft Defender will isolate undiscovered endpoints to block attacks

BleepingComputer - 11 April 2025 16:13

Microsoft is testing a new Defender for Endpoint capability that will block traffic to and from undiscovered endpoints to thwart attackers’ lateral network movement attempts. [...]

Palo Alto warns of brute-force login attempts on PAN-OS GlobalProtect gateways indicating possible upcoming attacks

Security Affairs - 11 April 2025 15:13

Experts warn of brute-force login attempts on PAN-OS GlobalProtect gateways following increased scanning activity on its devices. Palo Alto Networks reports brute-force login attempts on PAN-OS GlobalProtect gateways. The security firm pointed out that no known vulnerability has been exploited, but monitoring and analysis continue. “Our teams are observing evidence of activity consistent with password-related [...]

SpyNote, BadBazaar, MOONSHINE Malware Target Android and iOS Users via Fake Apps

The Hacker News - 11 April 2025 14:43

Cybersecurity researchers have found that threat actors are setting up deceptive websites hosted on newly registered domains to deliver a known Android malware called SpyNote.These bogus websites masquerade as Google Play Store install pages for apps like the Chrome web browser, indicating an attempt to deceive unsuspecting users into installing the malware instead.

Cybersecurity leaders discuss Oracle’s second recent hack

Security Magazine - 14 April 2025 02:00

Oracle has informed customers that a malicious actor accessed a computer system, stealing old login credentials for clients.

Paper Werewolf Threat Actor Targets Flash Drives With New Malware

darkreading - 11 April 2025 20:42

The threat actor, also known as Goffee, has been active since at least 2022 and has changed its tactics and techniques over the years while targeting Russian organizations.