Scottish Cyber Coordination Centre

Daily threat bulletin

22 November 2024

Vulnerabilities

Fortinet VPN design flaw hides successful brute-force attacks

BleepingComputer - 21 November 2024 10:38

A design flaw in the Fortinet VPN server's logging mechanism can be leveraged to conceal the successful verification of credentials during a brute-force attack without tipping off defenders of compromised logins. [...]

More than 2,000 Palo Alto Networks firewalls hacked exploiting recently patched zero-days

Security Affairs - 22 November 2024 07:24

Threat actors already hacked thousands of Palo Alto Networks firewalls exploiting recently patched zero-day vulnerabilities. Thousands of Palo Alto Networks firewalls have reportedly been compromised in attacks exploiting recently patched zero-day vulnerabilities (CVE-2024-0012 and CVE-2024-9474) in PAN-OS. CVE-2024-0012 is a vulnerability in Palo Alto Networks PAN-OS that allows unauthenticated attackers with network access to the management [...]

Google OSS-Fuzz Harnesses AI to Expose 26 Hidden Security Vulnerabilities

Infosecurity Magazine - 21 November 2024 15:45

One of these flaws detected using LLMs was in the widely used OpenSSL library

MITRE Updates List of 25 Most Dangerous Software Vulnerabilities

SecurityWeek - 21 November 2024 14:42

MITRE has released an updated CWE Top 25 Most Dangerous Software Weaknesses list, with cross-site scripting (XSS) at the top.

Threat actors and malware

Chinese hackers target Linux with new WolfsBane malware

BleepingComputer - 21 November 2024 16:06

A new Linux backdoor called 'WolfsBane' has been discovered, believed to be a port of Windows malware used by the Chinese 'Gelsemium' hacking group. [...]

NodeStealer Malware Targets Facebook Ad Accounts, Harvesting Credit Card Data

The Hacker News - 21 November 2024 13:04

Scottish Cyber Coordination Centre

Threat hunters are warning about an updated version of the Python-based NodeStealer that's now equipped to extract more information from victims' Facebook Ads Manager accounts and harvest credit card data stored in web browsers.

BianLian Ransomware Group Adopts New Tactics, Posing Significant Risk

Infosecurity Magazine - 21 November 2024 15:00

The BianLian ransomware group has shifted exclusively to exfiltration-based extortion and is deploying multiple new TTPs for initial access and persistence

Ransomhub ransomware gang claims the hack of Mexican government Legal Affairs Office

Security Affairs - 21 November 2024 22:06

Mexico is investigating a ransomware attack targeting its legal affairs office, as confirmed by the president amidst growing cybersecurity concerns. Mexico's president announced the government is investigating an alleged ransomware hack that targeted the administration's legal affairs office.

Chinese ship casts shadow over Baltic subsea cable snipfest

The Register - 21 November 2024 18:20

Danish military confirms it is monitoring as Swedish police investigate. Cloudflare says impact was 'minimal' The Danish military has confirmed it is tracking a Chinese ship that is under investigation after two optical fiber internet cables under the Baltic Sea were damaged....

After CrowdStrike Outage, Microsoft Debuts 'Quick Machine Recovery' Tool

SecurityWeek - 21 November 2024 15:20

Microsoft debuts Quick Machine Recovery tool to apply fixes even when machines are unable to boot, without needing physical access.