Scottish Cyber Coordination Centre

Daily Threat Bulletin

17 February 2025

Vulnerabilities

Attackers exploit recently disclosed Palo Alto Networks PAN-OS firewalls bug

Security Affairs - 15 February 2025 16:27

Threat actors are exploiting a recently disclosed vulnerability, tracked as CVE-2025-0108, in Palo Alto Networks PAN-OS firewalls. Researchers warn that threat actors are exploiting a recently disclosed vulnerability, tracked as CVE-2025-0108, in Palo Alto Networks PAN-OS firewalls. The Shadowserver Foundation researchers observed several CVE-2025-0108 attempts since 4 am UTC 2024-02-13 in their honeypots.

SonicWall Firewall Vulnerability Exploited After PoC Publication

SecurityWeek - 14 February 2025 13:25

The exploitation of a recent SonicWall vulnerability has started shortly after proof-of-concept (PoC) code was published.

New Windows Zero-Day Exploited by Chinese APT: Security Firm

SecurityWeek - 14 February 2025 12:40

ClearSky Cyber Security says it has seen a new Windows zero-day being exploited by a Chinese APT named Mustang Panda.

PostgreSQL flaw exploited as zero-day in BeyondTrust breach

BleepingComputer - 14 February 2025 10:15

Rapid7's vulnerability research team says attackers exploited a PostgreSQL security flaw as a zero-day to breach the network of privileged access management company BeyondTrust in December. [...]

New "whoAMI" Attack Exploits AWS AMI Name Confusion for Remote Code Execution

The Hacker News - 15 February 2025 01:12

Cybersecurity researchers have disclosed a new type of name confusion attack called whoAMI that allows anyone who publishes an Amazon Machine Image (AMI) with a specific name to gain code execution within the Amazon Web Services (AWS) account.

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-2024-57727 SimpleHelp Path Traversal Vulnerability.

Threat actors and malware

China-linked APT Salt Typhoon breached telecoms by exploiting Cisco router flaws

Security Affairs - 14 February 2025 20:23

China-linked APT Salt Typhoon has breached more U.S. telecommunications providers via unpatched Cisco IOS XE network devices. China-linked APT group Salt Typhoon is still targeting telecommunications providers worldwide, and according to a new report published by Recorded Future's Insikt Group, the threat actors has breached more U.S. telecommunications providers by exploiting unpatched Cisco IOS XE [...]

New FinalDraft malware abuses Outlook mail service for stealthy comms

BleepingComputer - 16 February 2025 11:15

A new malware called FinalDraft has been using Outlook email drafts for command-and-control communication in attacks against a ministry in a South American country. [...]

Lazarus Group Deploys Marstech1 JavaScript Implant in Targeted Developer Attacks

The Hacker News - 15 February 2025 00:58

The North Korean threat actor known as the Lazarus Group has been linked to a previously undocumented JavaScript implant named Marstech1 as part of limited targeted attacks against developers.

Russian Hackers Target Microsoft 365 Accounts with Device Code Phishing

Infosecurity Magazine - 14 February 2025 15:30

Volexity highlighted how Russian nation-state actors are stealing Microsoft device authentication codes to compromise accounts

RansomHub Becomes 2024's Top Ransomware Group, Hitting 600+ Organizations Globally

The Hacker News - 14 February 2025 16:47

The threat actors behind the RansomHub ransomware-as-a-service (RaaS) scheme have been observed leveraging now-patched security flaws in Microsoft Active Directory and the Netlogon protocol to escalate privileges and gain unauthorized access to a victim network's domain controller as part of their post-compromise strategy.