Scottish Cyber Coordination Centre

Daily threat bulletin

27 January 2025

Vulnerabilities

SonicWall warns of a critical CVE-2025-23006 zero-day likely exploited in the wild

Security Affairs - 24 January 2025 10:36

SonicWall warns customers of a critical zero-day vulnerability in SMA 1000 Series appliances, likely exploited in the wild. SonicWall is warning customers of a critical security vulnerability, tracked as CVE-2025-23006 (CVSS score of 9,8) impacting its Secure Mobile Access (SMA) 1000 Series appliances.

Cisco warns of a ClamAV bug with PoC exploit

Security Affairs - 26 January 2025 07:58

Cisco addressed a ClamAV denial-of-service (DoS) vulnerability, and experts warn of the availability of a proof-of-concept (PoC) exploit code. Cisco has released security updates to address a ClamAV denial-of-service (DoS) vulnerability tracked as CVE-2025-20128. The Cisco PSIRT experts warn of the availability of a proof-of-concept (PoC) exploit code for this flaw.

Meta's Llama Framework Flaw Exposes AI Systems to Remote Code Execution Risks

The Hacker News - 26 January 2025 16:45

A high-severity security flaw has been disclosed in Meta's Llama large language model (LLM) framework that, if successfully exploited, could allow an attacker to execute arbitrary code on the llama-stack inference server. The vulnerability, tracked as CVE-2024-50050, has been assigned a CVSS score of 6.3 out of 10.0.

Palo Alto Networks Addresses Impact of BIOS, Bootloader Vulnerabilities on Its Firewalls

SecurityWeek - 24 January 2025 12:20

Eclypsium warns that Palo Alto Networks firewalls are impacted by BIOS and bootloader flaws, but the vendor says users should not be concerned.

RANsacked: Over 100 Security Flaws Found in LTE and 5G Network Implementations

The Hacker News - 24 January 2025 19:28

A group of academics has disclosed details of over 100 security vulnerabilities impacting LTE and 5G implementations that could be exploited by an attacker to disrupt access to service and even gain a foothold into the cellular core network.

Microsoft: Outdated Exchange servers fail to auto-mitigate security bugs

BleepingComputer - 24 January 2025 11:26

Scottish Cyber Coordination Centre

Microsoft says outdated Exchange servers cannot receive new emergency mitigation definitions because an Office Configuration Service certificate type is being deprecated. [...]

Threat actors and malware

Ransomware gang uses SSH tunnels for stealthy VMware ESXi access

BleepingComputer - 26 January 2025 11:19

Ransomware actors targeting ESXi bare metal hypervisors are leveraging SSH tunneling to persist on the system while remaining undetected. [...]

J-magic malware campaign targets Juniper routers

Security Affairs - 24 January 2025 20:35

Threat actors are targeting Juniper routers with a custom backdoor in a campaign called code-named “J-magic,” attackers are exploiting a Magic Packet flaw. Lumen Technologies researchers reported that the J-magic campaign targets Juniper routers with a custom backdoor using a passive agent based on the cd00r variant (an open-source backdoor by fx).

Hackers use Windows RID hijacking to create hidden admin account

BleepingComputer - 24 January 2025 13:25

A North Korean threat group has been using a technique called RID hijacking that tricks Windows into treating a low-privileged account as one with administrator permissions. [...]

MintsLoader Delivers StealC Malware and BOINC in Targeted Cyber Attacks

The Hacker News - 27 January 2025 13:46

Threat hunters have detailed an ongoing campaign that leverages a malware loader called MintsLoader to distribute secondary payloads such as the StealC information stealer and a legitimate open-source network computing platform called BOINC.

Ransomware Gangs Linked by Shared Code and Ransom Notes

Infosecurity Magazine - 24 January 2025 10:15

SentinelOne researchers highlighted similarities in the approaches used by the HellCat and Morpheus ransomware groups, suggesting shared infrastructure

UK related

TalkTalk investigates breach after data for sale on hacking forum

BleepingComputer - 25 January 2025 17:23

UK telecommunications company TalkTalk is investigating a third-party supplier data breach after a threat actor began selling alleged customer data on a hacking forum. [...]

AWS Announces £5m Grant for Cyber Education in the UK

Scottish Cyber Coordination Centre

Infosecurity Magazine - 24 January 2025 15:30

Amazon Web Services has launched its Cyber Education Grant Program in the UK