Scottish
Cyber
Coordination
Centre

Daily threat bulletin

30 January 2025

Vulnerabilities

Attackers actively exploit a critical zero-day in Zyxel CPE Series devices

Security Affairs - 29 January 2025 11:17

Experts warn that threat actors are actively exploiting critical zero-day vulnerability, tracked as CVE-2024-40891, in Zyxel CPE Series devices. GreyNoise researchers are observing active exploitation attempts targeting a zero-day, tracked as CVE-2024-40891, in Zyxel CPE Series devices. The vulnerability is a command injection issue that remains unpatched and has not yet been publicly disclosed.

Rockwell Patches Critical, High-Severity Vulnerabilities in Several Products

SecurityWeek - 29 January 2025 12:22

Rockwell Automation has released six new security advisories to inform customers about several critical and high-severity vulnerabilities.

Critical remote code execution bug found in Cacti framework

Security Affairs - 29 January 2025 15:17

A critical flaw in Cacti open-source network monitoring and fault management framework that could allow remote code execution. Cacti is an open-source platform that provides a robust and extensible operational monitoring and fault management framework for users.

Laravel admin package Voyager vulnerable to one-click RCE flaw

BleepingComputer - 29 January 2025 15:27

Three vulnerabilities discovered in the open-source PHP package Voyager for managing Laravel applications could be used for remote code execution attacks. [...]

New Aquabot Botnet Exploits CVE-2024-41710 in Mitel Phones for DDoS Attacks

The Hacker News - 30 January 2025 13:11

A Mirai botnet variant dubbed Aquabot has been observed actively attempting to exploit a medium-severity security flaw impacting Mitel phones in order to ensnare them into a network capable of mounting distributed denial-of-service (DDoS) attacks.

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, as confirmed by Fortinet - CVE-2025-24085 Apple Multiple Products Use-After-Free Vulnerability.

Threat actors and malware

DeepSeek: What to know about the Chinese artificial intelligence model

Security Magazine - 29 January 2025 10:00

Cyber experts delve into DeepSeek, the Chinese artificial intelligence model.

Lazarus Group Uses React-Based Admin Panel to Control Global Cyber Attacks

The Hacker News - 29 January 2025 23:26

The North Korean threat actor known as the Lazarus Group has been observed leveraging a “web-based administrative platform” to oversee its command-and-control (C2) infrastructure, giving the adversary the ability to centrally supervise all aspects of their campaigns.

New Hellcat Ransomware Gang Employs Humiliation Tactics

Infosecurity Magazine - 29 January 2025 15:45

Cato Networks highlighted how the recently emerged HellCat ransomware group is using novel psychological tactics to court attention and pressurize victims

How Interlock Ransomware Infects Healthcare Organizations

The Hacker News - 29 January 2025 17:00

Ransomware attacks have reached an unprecedented scale in the healthcare sector, exposing vulnerabilities that put millions at risk. Recently, UnitedHealth revealed that 190 million Americans had their personal and healthcare data stolen during the Change Healthcare ransomware attack, a figure that nearly doubles the previously disclosed total.

FBI seizes Cracked.io, Nulled.to hacking forums in Operation Talent

BleepingComputer - 29 January 2025 13:30

The FBI has seized the domains for the infamous Cracked.io and Nulled.to hacking forums, which are known for their focus on cybercrime, password theft, cracking, and credential stuffing attacks. [...]

UK related

Scores of Critical UK Government IT Systems Have Major Security Holes

Infosecurity Magazine - 29 January 2025 10:30

The National Audit Office warns of major gaps in cyber resilience across UK government departments