Scottish Cyber Coordination Centre

Daily threat bulletin

19 November 2024

Vulnerabilities

Urgent: Critical WordPress Plugin Vulnerability Exposes Over 4 Million Sites

The Hacker News - 18 November 2024 11:22

A critical authentication bypass vulnerability has been disclosed in the Really Simple Security (formerly Really Simple SSL) plugin for WordPress that, if successfully exploited, could grant an attacker to remotely gain full administrative access to a susceptible site.The vulnerability, tracked as CVE-2024-10924 (CVSS score: 9.8), impacts both free and premium versions of the plugin.

Critical RCE bug in VMware vCenter Server now exploited in attacks

BleepingComputer - 18 November 2024 14:54

Broadcom warned today that attackers are now exploiting two VMware vCenter Server vulnerabilities, one of which is a critical remote code execution flaw. [...]

Fortinet VPN Zero-Day Exploited in Malware Attacks Remains Unpatched: Report

SecurityWeek - 18 November 2024 13:12

The DeepData malware framework was seen exploiting a Fortinet VPN client for Windows zero-day that remains unpatched.

Palo Alto Networks patches two firewall zero-days used in attacks

BleepingComputer - 18 November 2024 16:50

Palo Alto Networks has finally released security updates for an actively exploited zero-day vulnerability in its Next-Generation Firewalls (NGFW).

Threat actors and malware

Akira Ransomware Racks Up 30+ Victims in a Single Day

darkreading - 18 November 2024 20:49

Of the numerous victims, at least three refused to pay the demanded ransom, with the rest seemingly in talks with the cybercriminal group.

New Stealthy BabbleLoader Malware Spotted Delivering WhiteSnake and Meduza Stealers

The Hacker News - 18 November 2024 23:18

Scottish Cyber Coordination Centre

Cybersecurity researchers have shed light on a new stealthy malware loader called BabbleLoader that has been observed in the wild delivering information stealer families such as WhiteSnake and Meduza.BabbleLoader is an “extremely evasive loader, packed with defensive mechanisms, that is designed to bypass antivirus and sandbox environments to deliver stealers into memory.

Discontinued GeoVision Products Targeted in Botnet Attacks via Zero-Day

SecurityWeek - 18 November 2024 15:29

A zero-day vulnerability affecting five discontinued GeoVision product models has been exploited by a botnet.