Scottish
Cyber
Coordination
Centre

Daily threat bulletin

15 January 2025

Vulnerabilities

CVE-2024-55591: Fortinet Authentication Bypass Zero-Day Vulnerability Exploited in the Wild

Security Boulevard - 14 January 2025 21:00

Fortinet patched a zero day authentication bypass vulnerability in FortiOS and FortiProxy that has been actively exploited in the wild as a zero-day since November 2024.BackgroundOn January 14, Fortinet released a security advisory (FG-IR-24-535) addressing a critical severity vulnerability impacting FortiOS and FortiProxy.

Microsoft January 2025 Patch Tuesday fixes 8 zero-days, 159 flaws

BleepingComputer - 14 January 2025 15:01

Today is Microsoft's January 2025 Patch Tuesday, which includes security updates for 159 flaws, including eight zero-day vulnerabilities, with three actively exploited in attacks. [...]

Adobe: Critical Code Execution Flaws in Photoshop

SecurityWeek - 14 January 2025 21:03

Patch Tuesday: Adobe ships patches for more than a dozen security defects in a wide range of software products.

Critical SimpleHelp Flaws Allow File Theft, Privilege Escalation, and RCE Attacks

The Hacker News - 15 January 2025 11:40

Cybersecurity researchers have disclosed multiple security flaws in SimpleHelp remote access software that could lead to information disclosure, privilege escalation, and remote code execution.

Google OAuth flaw lets attackers gain access to abandoned accounts

BleepingComputer - 14 January 2025 13:28

A weakness in Google's OAuth "Sign in with Google" feature could enable attackers that register domains of defunct startups to access sensitive data of former employee accounts linked to various software-as-a-service (SaaS) platforms. [...]

Apple Bug Allows Root Protections Bypass Without Physical Access

darkreading - 14 January 2025 22:45

Emergent macOS vulnerability lets adversaries circumvent Apple's System Integrity Protection (SIP) by loading third-party kernels.

Threat actors and malware

WP3.XYZ malware attacks add rogue admins to 5,000+ WordPress sites

BleepingComputer - 14 January 2025 16:54

A new malware campaign has compromised more than 5,000 WordPress sites to create admin accounts, install a malicious plugin, and steal data. [...]

Russia-linked APT UAC-0063 target Kazakhstan in with HATVIBE malware

Security Affairs - 14 January 2025 17:29

Russia-linked threat actor UAC-0063 targets Kazakhstan to gather economic and political intelligence in Central Asia. Russia-linked threat actors UAC-0063 is targeting Kazakhstan as part of a cyber espionage campaign to gather economic and political intelligence in Central Asia.

Hackers use FastHTTP in new high-speed Microsoft 365 password attacks

BleepingComputer - 14 January 2025 11:57

Threat actors are utilizing the FastHTTP Go library to launch high-speed brute-force password attacks targeting Microsoft 365 accounts globally. [...]

Browser-Based Cyber-Threats Surge as Email Malware Declines

Infosecurity Magazine - 14 January 2025 16:00

Browser-based cyber-threats surged in 2024, with credential abuse and infostealers on the rise

FBI Wraps Up Eradication Effort of Chinese 'PlugX' Malware

darkreading - 14 January 2025 22:24

Two hacker groups were paid to develop malware targeting victims in the US, Europe, and Asia, as well as various Chinese dissident groups.

UK related

It's not just Big Tech: The UK's Online Safety Act applies across the board

The Register - 14 January 2025 13:15

A little more than two months out from its first legal deadline, the UK's Online Safety Act is causing concern among smaller online forums caught within its reach.

UK Considers Ban on Ransomware Payments by Public Bodies

Infosecurity Magazine - 14 January 2025 12:30

A UK government consultation has proposed banning public sector and critical infrastructure organizations from making ransomware payments to disincentivize attackers from targeting these services