Scottish
Cyber
Coordination
Centre

Daily threat bulletin

9 January 2025

Vulnerabilities

Ivanti Flaw CVE-2025-0282 Actively Exploited, Impacts Connect Secure and Policy Secure

The Hacker News - 09 January 2025 11:10

Ivanti is warning that a critical security flaw impacting Ivanti Connect Secure, Policy Secure, and ZTA Gateways has come under active exploitation in the wild beginning mid-December 2024.The security vulnerability in question is CVE-2025-0282 (CVSS score: 9.0), a stack-based buffer overflow that affects Ivanti Connect Secure before version 22.7R2.5, Ivanti Policy Secure before version 22.7R1.2

Hackers exploit KerioControl firewall flaw to steal admin CSRF tokens

BleepingComputer - 08 January 2025 14:55

Hackers are trying to exploit CVE-2024-52875, a critical CRLF injection vulnerability that leads to 1-click remote code execution (RCE) attacks in GFI KerioControl firewall product. [...]

Scammers Exploit Microsoft 365 to Target PayPal Users

Infosecurity Magazine - 08 January 2025 15:00

A new PayPal phishing scam used genuine money requests, bypassing security checks to deceive recipients

Unpatched critical flaws impact Fancy Product Designer WordPress plugin

BleepingComputer - 08 January 2025 17:34

Premium WordPress plugin Fancy Product Designer from Radykal is vulnerable to two critical severity flaws that remain unfixed in the current latest version. [...]

SonicWall warns of an exploitable SonicOS vulnerability

Security Affairs - 09 January 2025 00:09

SonicWall warns customers to address an authentication bypass vulnerability in its firewall’s SonicOS that is “susceptible to actual exploitation.” SonicWall is urging customers to upgrade the SonicOS firmware of their firewalls to patch an authentication bypass vulnerability tracked as CVE-2024-53704 (CVSS score of 8.2).

Chrome 131, Firefox 134 Updates Patch High-Severity Vulnerabilities

SecurityWeek - 08 January 2025 12:00

Chrome and Firefox updates released this week resolve high-severity vulnerabilities in the two popular browsers.

Threat actors and malware

Mirai Botnet Variant Exploits Four-Faith Router Vulnerability for DDoS Attacks

The Hacker News - 08 January 2025 16:59

A Mirai botnet variant has been found exploiting a newly disclosed security flaw impacting Four-Faith industrial routers since early November 2024 with the goal of conducting distributed denial-of-service (DDoS) attacks.The botnet maintains approximately 15,000 daily active IP addresses, with the infections primarily scattered across China, Iran, Russia, Turkey, and the United States.

Gayfemboy Botnet targets Four-Faith router vulnerability

Security Affairs - 08 January 2025 20:09

Gayfemboy, a Mirai botnet variant, has been exploiting a flaw in Four-Faith industrial routers to launch DDoS attacks since November 2024. The Gayfemboy botnet was first identified in February 2024, it borrows the code from the basic Mirai variant and now integrates N-day and 0-day exploits. By November 2024, Gayfemboy exploited 0-day vulnerabilities in Four-Faith [...]

Top 5 Malware Threats to Prepare Against in 2025

The Hacker News - 08 January 2025 17:32

2024 had its fair share of high-profile cyber attacks, with companies as big as Dell and TicketMaster falling victim to data breaches and other infrastructure compromises. In 2025, this trend will continue. So, to be prepared for any kind of malware attack, every organization needs to know its cyber enemy in advance. Here are 5 common malware families that you can start preparing to counter

Russian ISP confirms Ukrainian hackers “destroyed” its network

BleepingComputer - 08 January 2025 15:26

Russian internet service provider Nodex confirmed on Tuesday that its network was “destroyed” in a cyberattack claimed by Ukrainian hacktivists part of the Ukrainian Cyber Alliance [...]