Scottish Cyber Coordination Centre

Daily threat bulletin

12 February 2025

Vulnerabilities

Attackers exploit a new zero-day to hijack Fortinet firewalls

Security Affairs - 12 February 2025 00:06

Fortinet warned of attacks using a now-patched zero-day vulnerability in FortiOS and FortiProxy to hijack Fortinet firewalls. Fortinet warned that threat actors are exploiting a new zero-day vulnerability, tracked as CVE-2025-24472 (CVSS score of 8.1), in FortiOS and FortiProxy to hijack Fortinet firewalls.

Ivanti Patches Critical Flaws in Connect Secure and Policy Secure – Update Now

The Hacker News - 12 February 2025 12:27

Ivanti has released security updates to address multiple security flaws impacting Connect Secure (ICS), Policy Secure (IPS), and Cloud Services Application (CSA) that could be exploited to achieve arbitrary code execution.

High-Severity OpenSSL Vulnerability Found by Apple Allows MitM Attacks

SecurityWeek - 11 February 2025 19:07

OpenSSL has patched CVE-2024-12797, a high-severity vulnerability found by Apple that can allow man-in-the-middle attacks.

Progress Software Patches High-Severity LoadMaster Flaws Affecting Multiple Versions

The Hacker News - 11 February 2025 18:22

Progress Software has addressed multiple high-severity security flaws in its LoadMaster software that could be exploited by malicious actors to execute arbitrary system commands or download any file from the system.

SonicWall firewall exploit lets hackers hijack VPN sessions, patch now

BleepingComputer - 11 February 2025 11:56

Security researchers at Bishop Fox have published complete exploitation details for the CVE-2024-53704 vulnerability that allows bypassing the authentication mechanism in certain versions of the SonicOS SSLVPN application. [...]

Microsoft February 2025 Patch Tuesday fixes 4 zero-days, 55 flaws

BleepingComputer - 11 February 2025 14:56

Today is Microsoft's February 2025 Patch Tuesday, which includes security updates for 55 flaws, including four zero-day vulnerabilities, with two actively exploited in attacks. [...]

Scottish Cyber Coordination Centre

CISA Adds Four Known Exploited Vulnerabilities to Catalog

CISA Advisories -

CISA has added four vulnerabilities to its Known Exploited Vulnerabilities Catalog, based on evidence of active exploitation; CVE-2024-40891 Zyxel DSL CPE OS Command Injection Vulnerability; CVE-2024-40890 Zyxel DSL CPE OS Command Injection Vulnerability; CVE-2025-21418 Microsoft Windows Ancillary Function Driver for WinSock Heap-Based Buffer Overflow Vulnerability; CVE-2025-21391 Microsoft Windows Storage Link Following Vulnerability.

Threat actors and malware

Threat Actors Exploit ClickFix to Deploy NetSupport RAT in Latest Cyber Attacks

The Hacker News - 11 February 2025 16:25

Threat actors have observed the increasingly common ClickFix technique to deliver a remote access trojan named NetSupport RAT since early January 2025.NetSupport RAT, typically propagated via bogus websites and fake browser updates, grants attackers full control over the victim's host.

New Chinese Hacking Campaign Targets Manufacturing Firms to Steal IP

Infosecurity Magazine - 11 February 2025 17:15

Chinese hackers are infiltrating the networks of suppliers of "sensitive" manufacturers, according to a Check Point report to be published in the coming weeks

Authorities Disrupt 8Base Ransomware, Arrest Four Russian Operators

SecurityWeek - 11 February 2025 14:52

Law enforcement agencies take down the 8Base ransomware group's infrastructure, arrest four Russian operators.