Scottish Cyber Coordination Centre

Daily Threat Bulletin

3 November 2025

Vulnerabilities

Old Linux Kernel flaw CVE-2024-1086 resurfaces in ransomware attacks

Security Affairs - 31 October 2025 19:11

CISA warns ransomware gangs exploit CVE-2024-1086, a Linux kernel flaw in netfilter: nf_tables, introduced in 2014 and patched in Jan 2024. CISA warned that ransomware gangs are exploiting CVE-2024-1086, a high-severity Linux kernel flaw introduced in 2014 and patched in January 2024.

U.S. CISA adds XWiki Platform, and Broadcom VMware Aria Operations and VMware Tools flaws to its Known Exploited Vulnerabilities catalog

Security Affairs - 31 October 2025 00:14

U.S. Cybersecurity and Infrastructure Security Agency (CISA) adds XWiki Platform, and Broadcom VMware Aria Operations and VMware Tools flaws to its Known Exploited Vulnerabilities catalog.

Critical Claroty Authentication Bypass Flaw Opened OT to Attack

darkreading - 30 October 2025 21:29

CVE-2025-54603 gave attackers an opening to disrupt critical operational technology (OT) environments and critical infrastructure, plus steal data from them.

Scans for Port 8530/8531 (TCP). Likely related to WSUS Vulnerability CVE-2025-59287, (Sun, Nov 2nd)

SANS Internet Storm Centre - 02 November 2025 18:50

Sensors reporting firewall logs detected a significant increase in scans for port 8530/TCP and 8531/TCP over the course of last week. Some of these reports originate from Shadowserver, and likely other researchers, but there are also some that do not correspond to known research-related IP addresses.

Threat actors and malware

China-linked hackers exploited Lanscope flaw as a zero-day in attacks

BleepingComputer - 01 November 2025 11:16

China-linked cyber-espionage actors tracked as ‘Bronze Butler’ (Tick) exploited a Motex Lanscope Endpoint Manager vulnerability as a zero-day to deploy an updated version of their Gokcpdoor malware. [...]

Scottish Cyber Coordination Centre

Alleged Meduza Stealer malware admins arrested after hacking Russian org

BleepingComputer - 31 October 2025 10:45

The Russian authorities have arrested three individuals in Moscow who are believed to be the creators and operators of the Meduza Stealer information-stealing malware. [...]

BadCandy Webshell threatens unpatched Cisco IOS XE devices, warns Australian government

Security Affairs - 01 November 2025 18:41

Australia warns of attacks on unpatched Cisco IOS XE devices exploiting CVE-2023-20198, allowing BadCandy webshell install. The Australian Signals Directorate (ASD) warns of ongoing attacks on unpatched Cisco IOS XE devices exploiting CVE-2023-20198, allowing BadCandy webshell infections and admin takeover.

Suspected Chinese actors compromise U.S. Telecom firm Ribbon Communications

Security Affairs - 31 October 2025 09:52

A nation-state actor, likely a China-nexus one, hacked the U.S.-based technology company Ribbon Communications. Ribbon Communications is a U.S.-based technology company that provides telecommunications and networking. Ribbon Communications employs approximately 3,052 people as of December 31, 2024.

Russian Ransomware Gangs Weaponize Open-Source AdaptixC2 for Advanced Attacks

The Hacker News - 30 October 2025 23:10

The open-source command-and-control (C2) framework known as AdaptixC2 is being used by a growing number of threat actors, some of whom are related to Russian ransomware gangs.AdaptixC2 is an emerging extensible post-exploitation and adversarial emulation framework designed for penetration testing.

LotL Attack Hides Malware in Windows Native AI Stack

darkreading - 30 October 2025 20:47

Security programs trust AI data files, but they shouldn't: they can conceal malware more stealthily than most file types.

Suspected Chinese snoops weaponize unpatched Windows flaw to spy on European diplomats

The Register - 30 October 2025 20:20

Expired security cert, real Brussels agenda, plus PlugX malware finish the job Cyber spies linked to the Chinese government exploited a Windows shortcut vulnerability disclosed in March – but that Microsoft hasn't fixed yet – to target European diplomats in an effort to steal defense and national security details.

Ukrainian Man Extradited From Ireland to US Over Conti Ransomware Charges

SecurityWeek - 31 October 2025 14:20

Scottish Cyber Coordination Centre

Oleksii Oleksiyovych Lytvynenko is now in the US after being held in custody in Ireland since 2023.