Scottish
Cyber
Coordination
Centre

Daily Threat Bulletin

06 February 2025

Vulnerabilities

CISA orders agencies to patch Linux kernel bug exploited in attacks

BleepingComputer - 05 February 2025 14:58

CISA has ordered federal agencies to secure their systems within three weeks against a high-severity Linux kernel flaw actively exploited in attacks.

U.S. CISA adds Microsoft .NET Framework, Apache OFBiz, and Paessler PRTG Network Monitor flaws to its Known Exploited Vulnerabilities catalog

Security Affairs - 05 February 2025 16:02

U.S. Cybersecurity and Infrastructure Security Agency (CISA) adds Microsoft .NET Framework, Apache OFBiz, and Paessler PRTG Network Monitor flaws to its Known Exploited Vulnerabilities catalog.

New Veeam Flaw Allows Arbitrary Code Execution via Man-in-the-Middle Attack

The Hacker News - 05 February 2025 18:46

Veeam has released patches to address a critical security flaw impacting its Backup software that could allow an attacker to execute arbitrary code on susceptible systems. The vulnerability, tracked as CVE-2025-23114, carries a CVSS score of 9.0 out of 10.0.

Chrome 133, Firefox 135 Patch High-Severity Vulnerabilities

SecurityWeek - 05 February 2025 12:41

Chrome 133 and Firefox 135 were released with patches for multiple high-severity memory safety vulnerabilities.

Threat actors and malware

Hackers spoof Microsoft ADFS login pages to steal credentials

BleepingComputer - 05 February 2025 14:41

A help desk phishing campaign targets an organization's Microsoft Active Directory Federation Services (ADFS) using spoofed login pages to steal credentials and bypass multi-factor authentication (MFA) protections.

AsyncRAT Campaign Uses Python Payloads and TryCloudflare Tunnels for Stealth Attacks

The Hacker News - 05 February 2025 16:10

A malware campaign has been observed delivering a remote access trojan (RAT) named AsyncRAT by making use of Python payloads and TryCloudflare tunnels.

Abandoned Amazon S3 Buckets Enabled Attacks Against Governments, Big Firms

SecurityWeek - 05 February 2025 13:45

150 abandoned Amazon S3 buckets could have been leveraged to deliver malware or backdoors to governments and Fortune companies.

Silent Lynx Using PowerShell, Golang, and C++ Loaders in Multi-Stage Cyberattacks

The Hacker News - 05 February 2025 19:16

A previously undocumented threat actor known as Silent Lynx has been linked to cyber attacks targeting various entities in Kyrgyzstan and Turkmenistan. This threat group has previously targeted entities around Eastern Europe and Central Asian.