Scottish Cyber Coordination Centre

Daily threat bulletin

17 December 2024

Vulnerabilities

Windows kernel bug now exploited in attacks to gain SYSTEM privileges

BleepingComputer - 16 December 2024 15:50

CISA has warned U.S. federal agencies to secure their systems against ongoing attacks targeting a high-severity Windows kernel vulnerability. [...]

Android Zero-Day Exploited in Spyware Campaigns, Amnesty International Points to Cellebrite

SecurityWeek - 16 December 2024 18:59

Israeli forensics firm Cellebrite has been linked to an Android zero-day used to secretly install spyware on Serbian journalists' phones.

Undocumented DrayTek Vulnerabilities Exploited to Hack Hundreds of Orgs

SecurityWeek - 16 December 2024 15:17

Undocumented vulnerabilities in DrayTek devices were exploited in ransomware campaigns that compromised over 300 organizations.

CVE Assigned to Cleo Vulnerability as Cl0p Ransomware Group Takes Credit for Exploitation

SecurityWeek - 16 December 2024 14:13

The Cl0p ransomware group has taken credit for exploitation of the Cleo product vulnerability tracked as CVE-2024-55956.

CISA Adds Two Known Exploited Vulnerabilities to Catalog

CISA Advisories -

CISA has added two new vulnerabilities to its Known Exploited Vulnerabilities Catalog, based on evidence of active exploitation - CVE-2024-20767 Adobe ColdFusion Improper Access Control Vulnerability, CVE-2024-35250 Microsoft Windows Kernel-Mode Driver Untrusted Pointer Dereference Vulnerability.

Threat actors and malware

Citrix Warns of Password Spraying Attacks Targeting NetScaler Appliances

SecurityWeek - 16 December 2024 15:53

Scottish Cyber Coordination Centre

Citrix issues warning on password spraying attacks targeting NetScaler and NetScaler Gateway appliances deployed by organizations worldwide.

The Mask APT Resurfaces with Sophisticated Multi-Platform Malware Arsenal

The Hacker News - 17 December 2024 13:25

A little-known cyber espionage actor known as The Mask has been linked to a new set of attacks targeting an unnamed organization in Latin America twice in 2019 and 2022.

CISA and FBI Raise Alerts on Exploited Flaws and Expanding HiatusRAT Campaign

The Hacker News - 17 December 2024 12:17

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) on Monday added two security flaws to its Known Exploited Vulnerabilities (KEV) catalog, citing evidence of active exploitation in the wild.

Fake Captcha Campaign Highlights Risks of Malvertising Networks

Infosecurity Magazine - 16 December 2024 15:00

Large-scale campaign identified by Guardio Lans and Infoblox, exploiting malvertising and fake captchas to distribute Lumma infostealer for massive theft

Dark web threats and dark market predictions for 2025

Securelist - 16 December 2024 11:00

Kaspersky experts review dark market trends in 2024, such as popularity of cryptors, loaders and crypto drainers on the dark web, and discuss what to expect in 2025.