Scottish Cyber Coordination Centre

TLP CLEAR: Disclosure is not limited

Daily threat summary

18 January 2024

Vulnerabilities

CISA Adds Three Known Exploited Vulnerabilities to Catalog

CISA Current Activity - January 17 2024

CISA has added three new vulnerabilities to its Known Exploited Vulnerabilities Catalog, based on evidence of active exploitation. CVE-2023-6549 Citrix NetScaler ADC and NetScaler Gateway Buffer Overflow Vulnerability CVE-2023-6548 Citrix NetScaler ADC and NetScaler Gateway Code Injection Vulnerability CVE-2024-0519 Google Chromium V8 Out-of-Bounds Memory Access Vulnerability.

CISA pushes federal agencies to patch Citrix RCE within a week

BleepingComputer.com - January 17 2024

Today, CISA ordered U.S. federal agencies to secure their systems against three recently patched Citrix NetScaler and Google Chrome zero-days actively exploited in attacks.

Google Chrome Zero-Day Bug Under Attack, Allows Code Injection

Dark Reading - January 17 2024

Google has patched a high-severity zero-day bug in its Chrome Web browser that attackers are actively exploiting. It paves the way for code execution and other cyberattacks on targeted endpoints. The vulnerability, assigned as CVE-2024-0519, is the first Chrome zero-day bug that Google has disclosed in 2024, and the second in the browser in less than a calendar month.

Oracle Critical Patch Update Advisory - January 2024

NCSC-FI Daily Vulnerabilities - January 18 2024

This Critical Patch Update contains 389 new security patches across the product families listed below.

Nearly 7K WordPress Sites Compromised by Balada Injector

Dark Reading - January 17 2024

Scottish Cyber Coordination Centre

TLP CLEAR: Disclosure is not limited

Nearly 200K WordPress sites could be vulnerable to the attack thanks to CVE-2023-6000, lurking in the PopUp Builder plug-in.

Ransomware

LockBit Ransomware Distributed Via Word Files Disguised as Resumes

ASEC Blog - AhnLab English - January 18 2024

AhnLab Security intelligence Center (ASEC) has identified that LockBit ransomware is being distributed via Word files since last month. A notable point is that the LockBit ransomware is usually distributed by disguising itself as resumes, and recently found malicious Word files were also disguised as resumes.

Malware and threat actors

Botnet fuels Androxgh0st malware's punch

SC Magazine US - January 17 2024

Threat actors responsible for the multi-faceted Androxgh0st malware have built a botnet to expand their capabilities to identify and exploit vulnerable networks. In a joint Jan. 16 advisory, the Cybersecurity and Infrastructure Security Agency (CISA) and the FBI revealed new details about the malware which they said was gleaned from their involvement in multiple, ongoing investigations.

New iShutdown Method Exposes Hidden Spyware Like Pegasus on Your iPhone

The Hacker News - January 17 2024

Cybersecurity researchers have identified a "lightweight method" called iShutdown for reliably identifying signs of spyware on Apple iOS devices, including notorious threats like NSO Group's Pegasus, QuaDream's Reign, and Intellexa's Predator.

Bigpanzi botnet infects 170,000 Android TV boxes with malware

Bleeping Computer - January 17 2024

A previously unknown cybercrime syndicate named 'Bigpanzi' has been making significant money by infecting Android TV and eCos set-top boxes worldwide since at least 2015. Beijing-based Qianxin Xlabs reports that the threat group controls a large-scale botnet of approximately 170,000 daily active bots.