Scottish
Cyber
Coordination
Centre

TLP CLEAR: Disclosure is not limited

Daily threat summary

5 February 2024

Vulnerabilities

Mastodon Vulnerability Allows Hackers to Hijack Any Decentralized Account

The Hacker News - February 3 2024

The decentralized social network Mastodon has disclosed a critical security flaw that enables malicious actors to impersonate and take over any account. "Due to insufficient origin validation in all Mastodon, attackers can impersonate and take over any remote account," the maintainers said in a terse advisory.

ThreatLabz Coverage Advisory: Ivant's VPN Vulnerabilities Exploited by Hackers, New Zero-Days Pose Critical Risk

Tech-Wreck InfoSec Blog - February 4 2024

Introduction Ivanti, an IT management and security company, has issued a warning about multiple zero-day vulnerabilities in its VPN products exploited by Chinese state-backed hackers since December 2023. The initial disclosure involved two CVEs (CVE-2023-46805 and CVE-2023-21887) allowing a remote attacker to perform authentication bypass and remote command injection exploits. Ivanti released a patch which was immediately bypassed by two additional flaws (CVE-2024-21888 and CVE-2024-21893) that allows an attacker to perform privilege escalation and server-side request forgery exploits.

Leaky Vessels flaws allow hackers to escape Docker, runc containers

Bleeping Computer - February 4 2024

Four vulnerabilities collectively called "Leaky Vessels" allow hackers to escape containers and access data on the underlying host operating system. The flaws were discovered by Snyk security researcher Rory McNamara in November 2023, who reported them to impacted parties for fixing. Snyk has found no signs of active exploitation of the Leaky Vessels flaws in the wild, but the publicity could change the exploitation status, so all impacted system admins are recommended to apply the available security updates as soon as possible.

Week in review: Windows Event Log zero-day, exploited critical Jenkins RCE flaw

Help Net Security - February 4 2024

Scottish
Cyber
Coordination
Centre

TLP CLEAR: Disclosure is not limited

Ransomware

More Ransomware Victims Are Declining to Pay Extortionists
DataBreachToday.eu - February 2 2024

While Average Falls Below 30%, We're Still Far From Seeing Criminal Profits Dry Up
The number of victims who opt to pay a ransom appears to have declined to a record low.

LockBit 3.0 Ransomware Targets Manchester Fertility Clinic
The Cyber Express - February 2 2024

Manchester Fertility, a renowned fertility clinic with a rich history offering IUI, ICSI, & IVF treatments, is allegedly under threat from the notorious LockBit 3.0 ransomware group.

Malware and threat actors

Google Play Used to Spread 'Patchwork' APT's Espionage Apps
Dark Reading - February 2 2024

The Indian state-sponsored cyberattackers lurked in Google's official app store, distributing a new RAT and spying on Pakistanis.

New Mispadu Banking Trojan Exploiting Windows SmartScreen Flaw
The Hacker News - February 5 2024

The threat actors behind the Mispadu banking Trojan have become the latest to exploit a now-patched Windows SmartScreen security bypass flaw to compromise users in Mexico. The attacks entail a new variant of the malware that was first observed in 2019, Palo Alto Networks Unit 42 said in a report published last week.