Scottish Cyber Coordination Centre

Daily threat bulletin

2 April 2024

Vulnerabilities

New Linux Bug Could Lead to User Password Leaks and Clipboard Hijacking

The Hacker News - 29 March 2024 17:19

Details have emerged about a vulnerability impacting the “wall” command of the util-linux package that could be potentially exploited by a bad actor to leak a user’s password or alter the clipboard on certain Linux distributions.The bug, tracked as CVE-2024-28085, has been codenamed WallEscape by security researcher Skyler Ferrante. It has been described as a case of improper

Cisco IOS Bugs Allow Unauthenticated, Remote DoS Attacks

darkreading - 28 March 2024 22:15

Several Cisco products, including IOS, IOS XE, and AP software, need patching against various high-risk security vulnerabilities.

Easy-to-use make-me-root exploit lands for recent Linux kernels. Get patching

The Register - 29 March 2024 22:43

CVE-2024-1086 turns the page tables on system admins A Linux privilege-escalation proof-of-concept exploit has been published that, according to the bug hunter who developed it, typically works effortlessly on kernel versions between at least 5.14 and 6.6.14. ...

Nvidia’s newborn ChatRTX bot patched for security bugs

The Register - 28 March 2024 16:33

Flaws enable privilege escalation and remote code execution Nvidia’s AI-powered ChatRTX app launched just six week ago but already has received patches for two security vulnerabilities that enabled attack vectors, including privilege escalation and remote code execution....

WallEscape’ Linux Vulnerability Leaks User Passwords

SecurityWeek - 01 April 2024 17:06

A vulnerability in util-linux, a core utilities package in Linux systems, allows attackers to leak user passwords and modify the clipboard.The post ‘WallEscape’ Linux Vulnerability Leaks User Passwords appeared first on SecurityWeek.

Update Chrome now! Google patches possible drive-by vulnerability

Malwarebytes - 28 March 2024 12:25

Google has released an update for Chrome to fix seven security vulnerabilities.

Hardware Vulnerability in Apple’s M-Series Chips

Schneier on Security - 28 March 2024 12:05

It’s yet another hardware side-channel attack:The threat resides in the chip’s data memory-dependent prefetcher, a hardware optimization that predicts the memory addresses of data that running code is likely to access in the near future. By loading the contents into the CPU cache before it’s actually needed, the DMP, as the feature is abbreviated, reduces latency between the main memory and the CPU, a common bottleneck in modern computing. DMPs are a relatively new phenomenon found only in M-series chips and Intel’s 13th-generation Raptor Lake microarchitecture, although older forms of prefetchers have been common for years…

CISA Adds One Known Exploited Vulnerability to Catalog

CISA Advisories -

CISA has added one new vulnerability to its Known Exploited Vulnerabilities Catalog, based on evidence of active exploitation. CVE-2023-24955 Microsoft SharePoint Server Code Injection Vulnerability.

Threat actors and malware

New Vultur malware version includes enhanced remote control and evasion capabilities

Security Affairs - 01 April 2024 15:32

Researchers detected a new version of the Vultur banking trojan for Android with enhanced remote control and evasion capabilities. Researchers from NCC Group discovered a new version of the Vultur banking trojan for Android that includes new enhanced remote control and evasion capabilities. Some of the new features implemented in this variant include the ability […]

Linux Version of DinodasRAT Spotted in Cyber Attacks Across Several Countries

The Hacker News - 28 March 2024 23:32

Scottish Cyber Coordination Centre

A Linux version of a multi-platform backdoor called DinodasRAT has been detected in the wild targeting China, Taiwan, Turkey, and Uzbekistan, new findings from Kaspersky reveal.DinodasRAT, also known as XDealer, is a C++-based malware that offers the ability to harvest a wide range of sensitive data from compromised hosts.In October 2023, Slovak cybersecurity firm ESET

TheMoon Malware Rises Again with Malicious Botnet for Hire

darkreading - 29 March 2024 19:06

Outdated SOHO routers and IoT devices being hijacked by TheMoon to operate an anonymous hacker botnet service called Faceless.

Suspected MFA Bombing Attacks Target Apple iPhone Users

darkreading - 28 March 2024 16:03

Several Apple device users have experienced recent incidents where they have received incessant password reset prompts and vishing calls from a number spoofing Apple's legitimate customer support line.

Lessons from a Ransomware Attack against the British Library

Schneier on Security - 29 March 2024 12:03

You might think that libraries are kind of boring, but this self-analysis of a 2023 ransomware and extortion attack against the British Library is anything but.