Scottish Cyber Coordination Centre

TLP CLEAR: Disclosure is not limited

Daily threat summary

19 January 2023

Vulnerabilities

Frequent critical flaws open MLFlow users to imminent threats

CSO Magazine - January 18 2024

MLFlow has emerged as the most-vulnerable open source machine learning framework with four highly critical (CVSS 10) vulnerabilities reported within 50 days, according to a Protect AI report. Protect AI's AI/ML bug bounty program, hunter AI, discovered these vulnerabilities within the MLFlow platform, which can allow Remote Code Execution (RCE), Arbitrary File Overwrite, and Local File Include.

Citrix NetScaler, Google Chrome zero-days added to CISA's exploited vulnerabilities catalog

SC Magazine US - January 18 2024

SiliconAngle reports that Intel, American Megatrends, and Phoenix Technologies have been confirmed to be impacted by nine vulnerabilities within the widely used Unified Extensible Firmware Interface firmware TianoCore EDK II dubbed "PixieFail," which could be exploited to enable denial-of-service attacks, data leaks, and DNS cache poisoning.

CISA Releases One Industrial Control Systems Advisory

CISA Current Activity - January 18 2024

CISA released one Industrial Control Systems (ICS) advisory on January 18, 2024. These advisories provide timely information about current security issues, vulnerabilities, and exploits surrounding ICS. ICSA-24-018-01 AVEVA PI Server CISA encourages users and administrators to review the newly released ICS advisory for technical details and mitigations.

Ransomware

TeamViewer abused to breach networks in new ransomware attacks

Bleeping Computer - January 18 2024

Scottish Cyber Coordination Centre

TLP CLEAR: Disclosure is not limited

Ransomware actors are again using TeamViewer to gain initial access to organization endpoints and attempt to deploy encryptors based on the leaked LockBit ransomware builder. TeamViewer is a legitimate remote access tool used extensively in the enterprise world, valued for its simplicity and capabilities.

Malware and threat actors

Dark Web Profile: Scattered Spider
SOCRadar - January 18 2024

One hacker collective continues to confound federal law enforcement and cybersecurity experts — the Scattered Spider. Known by a multitude of aliases such as Muddled Libra, UNC3944, Starfraud, and Octo Tempest, this hacking group has not only infiltrated major corporate networks like MGM Resorts and Caesars Entertainment but has done so with a bold audacity that leaves many wondering.

Stealthy New macOS Backdoor Hides on Chinese Websites
Dark Reading - January 18 2024

Modified malware from the Khepri open source project that shares similarities with the ZuRu data stealer harvests data and drops additional payloads.