Scottish
Cyber
Coordination
Centre

TLP CLEAR: Disclosure is not limited

Daily threat summary

25 January 2024

Vulnerabilities

Critical Jenkins CLI File Read Vulnerability Could Lead to RCE Attacks (CVE-2024-23897)

SOCRadar - January 24 2024

Jenkins, a Java-based open-source automation platform with an extensive plugin ecosystem and continuous integration capabilities, has recently disclosed a series of vulnerabilities affecting its deliverables. Among them, a critical vulnerability stands out, with the risk of leading to Remote Code Execution (RCE).

CISA Adds One Known Exploited Vulnerability to Catalog

CISA Current Activity - January 24 2024

CISA has added one new vulnerability to its Known Exploited Vulnerabilities Catalog, based on evidence of active exploitation: CVE-2023-22527 - Atlassian Confluence Data Center and Server Template Injection Vulnerability.

Mozilla Releases Security Updates for Thunderbird and Firefox

CISA Current Activity - January 24 2024

Mozilla has released security updates to address vulnerabilities in Thunderbird and Firefox. A cyber threat actor could exploit one of these vulnerabilities to take control of an affected system. CISA encourages users and administrators to review the following advisories and apply the necessary updates.

Zoho ManageEngine ADSelfService Plus Remote Code Execution Vulnerability (CVE-2024-0252)

Qualys Threat Protection - January 24 2024

Zoho addressed a vulnerability in the ManageEngine ADSelfService Plus, CVE-2024-0252. The vulnerability is given a critical severity and a CVSS score of 9.9.

Scottish Cyber Coordination Centre

TLP CLEAR: Disclosure is not limited

UK cyber

UK says AI will empower ransomware over the next two years

Bleeping Computer - January 24 2024

The United Kingdom's National Cyber Security Centre (NCSC) warns that artificial intelligence (AI) tools will have an adverse near-term impact on cybersecurity, helping escalate the threat of ransomware. The agency says cybercriminals already use AI for various purposes, and the phenomenon is expected to worsen over the next two years, helping increase the volume and severity of cyberattacks. The NCSC believes that AI will enable inexperienced threat actors, hackers-for-hire, and low-skilled hacktivists to conduct more effective, tailored attacks that would otherwise require significant time, technical knowledge, and operational effort. Most available large learning model (LLM) platforms, such as ChatGPT and Bing Chat, have safeguards that prevent the platform from creating malicious content.

Ransomware

Critical Auth Bypass in GoAnywhere MFT: Is It a New Ransomware Gateway? (CVE-2024-0204)

SOCRadar - January 24 2024

Fortra has disclosed a critical vulnerability in its GoAnywhere MFT (Managed File Transfer) software – an authentication bypass that poses a severe security risk. Upon its successful exploitation, attackers could establish a new admin user, potentially paving the way for additional malicious actions.

The 2024 Ransomware Threat Landscape

Symantec Enterprise Blogs - January 24 2024

Although we are just a few weeks into the new year, ransomware attacks – and their costly impact on today's enterprises – are already making headlines. According to our new report, published today by the Symantec Threat Hunter Team, part of Broadcom, "ransomware continues to be one of the most lucrative forms of cybercrime and, as such, remains a critical threat for organizations of all sizes."

Malware and threat actors

Federal judge rejects NSO's effort to dismiss Apple's Pegasus lawsuit

TLP CLEAR: Disclosure is not limited

Record by Recorded Future - January 24 2024

A federal judge has denied a motion from spyware maker NSO Group to dismiss an Apple lawsuit alleging the company’s powerful Pegasus tool has violated computer fraud laws and unfairly profited off of Apple and its customers, according to a court ruling.

Dark Web Profile: Malek Team

SOCRadar - January 24 2024

In recent months, the Malek Team, a hacker group with alleged links to Iran, has escalated its cyber offensive against key Israeli institutions, marking a significant uptick in digital threats within the region. The Malek Team, which has previously targeted a private college in Israel, claimed responsibility for a sophisticated cyberattack on Israel’s Ziv Medical Center.