Scottish
Cyber
Coordination
Centre

TLP CLEAR: Disclosure is not limited

Daily threat summary

29 January 2024

Vulnerabilities

Malicious PyPI Packages Slip WhiteSnake InfoStealer Malware onto Windows Machines

The Hacker News - January 29 2024

Cybersecurity researchers have identified malicious packages on the open-source Python Package Index (PyPI) repository that deliver an information stealing malware called WhiteSnake Stealer on Windows systems. The malware-laced packages are named nigpal, figflix, telerer, seGMM, fbdebug, sGMM, myGens, NewGends, and TestLibs111. They have been uploaded by a threat actor named "WS."

Critical RCE Vulnerability in Cisco Unified Communications with Risk of Root Access (CVE-2024-20253)

SOCRadar - January 26 2024

The Cybersecurity and Infrastructure Security Agency (CISA) has issued an alert highlighting Cisco security updates, which address a critical vulnerability. The vulnerability affects several Cisco Unified Communications and Contact Center Solutions products, potentially resulting in Remote Code Execution (RCE).

Exploits released for critical Jenkins RCE flaw, patch now

Bleeping Computer - January 28 2024

Multiple proof-of-concept (PoC) exploits for a critical Jenkins vulnerability allowing unauthenticated attackers to read arbitrary files have been made publicly available, with some researchers reporting attackers actively exploiting the flaws in attacks.

Malware and threat actors

The APT Files #2: Putter Panda

Medium Infosec Cybersecurity Writeups - RSS - January 28 2024

TLP CLEAR: Disclosure is not limited

Putter Panda is a threat group suspected to be under the military cover of Unit 61486 of the Chinese People’s Liberation Army (PLA). The origin of the group’s name is from its knack for targeting golf players (putter) and its origin (China).

Medusa ransomware attack hit Kansas City Area Transportation Authority

Security Affairs - January 28 2024

Medusa ransomware gang claimed responsibility for the attack against the Kansas City Area Transportation Authority (KCATA). On January 23, 2023, the Kansas City Area Transportation Authority (KCATA) suffered a ransomware attack. The Kansas City Area Transportation Authority (KCATA) is a public transit agency in metropolitan Kansas City.

PixPirate: The Brazilian financial malware you can’t see

Security Intelligence - January 28 2024

Malicious software always aims to stay hidden, making itself invisible so the victims can’t detect it. The constantly mutating PixPirate malware has taken that strategy to a new extreme. PixPirate is a sophisticated financial remote access trojan (RAT) malware that heavily utilizes anti-research techniques.