Scottish Cyber Coordination Centre

TLP CLEAR: Disclosure is not limited

Daily threat summary

12 February 2024

Vulnerabilities

JetBrains Releases Security Advisory for TeamCity On-Premises
CISA Current Activity - February 9 2024

JetBrains released a security advisory to address a vulnerability (CVE-2024-23917) in TeamCity On-Premises. A cyber threat actor could exploit this vulnerability to take control of an affected system. CISA encourages users and administrators to review the Critical Security Issue Affecting TeamCity On-Premises-CVE-2024-23917 and apply the necessary update or workarounds.

Raspberry Robin spotted using two new 1-day LPE exploits
Security Affairs - February 11 2024

Raspberry Robin continues to evolve, it was spotted using two new one-day exploits for vulnerabilities either Discord to host samples. Raspberry Robin is a Windows worm discovered by cybersecurity researchers from Red Canary, the malware propagates through removable USB devices. The malicious code uses Windows Installer to reach out to QNAP-associated domains and download a malicious DLL. The malware uses TOR exit nodes as a backup C2 infrastructure.

Fortinet Warns of New FortiOS Zero-Day
SecurityWeek RSS Feed - February 9 2024

Fortinet patches CVE-2024-21762, a critical remote code execution vulnerability that may have been exploited in the wild. The post Fortinet Warns of New FortiOS Zero-Day appeared first on SecurityWeek.

Ivanti Connect Secure and Ivanti Policy Secure XML eXternal Entity (XXE) Vulnerability (CVE-2024-22024)
Qualys Threat Protection - February 9 2024

Ivanti has warned users to patch an XML external entity vulnerability impacting Connect Secure, Policy Secure, and ZTA gateways. CVE-2024-22024 may allow an attacker to access certain restricted resources without authentication. Ivanti has mentioned in the...

Scottish Cyber Coordination Centre

TLP CLEAR: Disclosure is not limited

Malware and threat actors

MacOS Targeted by New Backdoor Linked to ALPHV Ransomware

Dark Reading - February 9 2024

Researchers have discovered a new backdoor targeting macOS that appears to have ties to an infamous ransomware family that historically targets Windows systems. Researchers at Bitdefender say the so-called Trojan[.]MAC[.]RustDoor is likely linked to BlackCat/ALPHV. The newly discovered backdoor is written in Rust coding language and impersonates an update for Visual Studio code editor. Bitdefender in its advisory said there have been multiple variants of the new backdoor, and that it has been in action for at least three months. The macOS malware gathers data from the Desktop and Documents folders, along with user notes, and then compresses the information into a ZIP archive and sends it to a command-and-control (C2) server.

Volt Typhoon lays low in Critical Infrastructure Networks

MalwareTips.com - February 10 2024

Hackers backed by China are breaking into the networks of US companies so they are able to launch destructive cyber attacks against critical infrastructure in the event of a major crisis or conflict. In their attempts to gain access to systems the attackers are paying particular attention to... Click to expand...
Read more