Scottish Cyber Coordination Centre

TLP CLEAR: Disclosure is not limited

Daily threat summary

7 February 2024

Vulnerabilities

JetBrains warns of new TeamCity auth bypass vulnerability

Bleeping Computer - February 6 2024

JetBrains urged customers today to patch their TeamCity On-Premises servers against a critical authentication bypass vulnerability that can let attackers take over vulnerable instances with admin privileges. Tracked as CVE-2024-23917, this critical severity flaw impacts all versions of TeamCity On-Premises from 2017.1 through 2023.11.2 and can be exploited in remote code execution (RCE) attacks that don't require user interaction. "We strongly advise all TeamCity On-Premises users to update their servers to 2023.11.3 to eliminate the vulnerability," JetBrains said.

CISA Adds One Known Exploited Vulnerability to Catalog

CISA Current Activity - February 6 2024

CISA has added one new vulnerability to its Known Exploited Vulnerabilities Catalog, based on evidence of active exploitation. CVE-2023-4762 Google Chromium V8 Type Confusion Vulnerability.

Windows SmartScreen bug targeted by new Mispadu trojan variant

SC Magazine US - February 6 2024

SecurityWeek reports that numerous Mitsubishi Electric factory automation products were disclosed to have been affected by serious security vulnerabilities, including a critical remote code execution flaw, tracked as CVE-2023-6943, and a high-severity authentication bypass vulnerability, tracked as CVE-2023-6942.

Critical vulnerability affecting most Linux distros allows for bootkits

ArsTechnica - February 7 2024

Enlarge Linux developers are in the process of patching a high-severity vulnerability that, in certain cases, allows the installation of malware that runs at the firmware level, giving infections access to the deepest parts of a device where they’re hard to detect or remove. The vulnerability affects shim, which in the context of Linux is a small component that runs in the firmware early in the boot process before the operating system has started.

TLP CLEAR: Disclosure is not limited

Google fixed an Android critical remote code execution flaw

Security Affairs - February 6 2024

Google released Android 's February 2024 security patches to address 46 vulnerabilities, including a critical remote code execution issue. Google released Android February 2024 security patches to address 46 vulnerabilities, including a critical remote code execution flaw tracked as CVE-2024-0031.

Malware and threat actors

Impact of CL0P Ransomware on the Cyber Threat Landscape in 2023: An Analysis of Cyber Tactics and Threat Evolution Over the Year

SOCRadar - February 6 2024

In the intricate web of cybersecurity threats, the CL0P ransomware group carved out a reputation for its sophisticated and strategic operations last year. This article aims to unpack the unique modus operandi of CL0P, contrasting it with other formidable players in the ransomware arena. Leveraging SOCRadar Cyber Intelligence's rich data repository, we reveal a year's worth of tactics, targets, and trends that set CL0P apart.

Identity Protection Action Items Following Midnight Blizzard Attack

Security Bloggers Network - February 6 2024

In light of the Midnight Blizzard's attack, it's evident that our cybersecurity strategies must evolve to keep pace with the sophisticated tactics employed by nation-state actors.

Chinese Hackers Penetrated Unclassified Dutch Network

DataBreachToday.eu - February 7 2024

Chinese espionage hackers penetrated Dutch military systems in early 2023, using a zero-day exploit in a Fortinet virtual private network to obtain access,