Scottish Cyber Coordination Centre

TLP CLEAR: Disclosure is not limited

Daily threat summary

20 February 2024

Vulnerabilities

CVE-2024-25710: Apache Commons Compress: Denial of service caused by an infinite loop for a corrupted DUMP file

Open Source Security - February 19 2024

Loop with Unreachable Exit Condition ('Infinite Loop') vulnerability in Apache Commons Compress[.]This issue affects Apache Commons Compress: from 1.3 through 1.25.0. Users are recommended to upgrade to version 1.26.0 which fixes the issue.

Hackers exploit critical RCE flaw in Bricks WordPress site builder

Bleeping Computer - February 19 2024

Hackers are actively exploiting a critical remote code execution (RCE) flaw impacting the Brick Builder Theme to run malicious PHP code on vulnerable sites. The Bricks Builder Theme is a premium WordPress theme described as an innovative, community-driven visual site builder. With around 25,000 active installations, the product promotes user friendliness and customization in website design.

Malware and threat actors

LockBit, the world's worst ransomware, is down

Malwarebytes Labs Blog - February 20 2024

For the last two years the absolute worst, most prolific, most globally significant "big game" ransomware gang has been LockBit. This evening its position as ransomware's biggest beast is suddenly in doubt, following some non-consensual website redecoration at the hands of the UK's National Crime Agency (NCA). The LockBit data leak site has a new look The LockBit dark web site usually hosts the names and data of organisations that refused to pay ransoms. That's been replaced by a message from the NCA, saying: This site is now under the control of The National Crime Agency of the UK, working in close cooperation with the FBI and the international law enforcement task force, 'Operation Cronos'.

Scottish Cyber Coordination Centre

TLP CLEAR: Disclosure is not limited

[North Korean hackers linked to defense sector supply-chain attack]

Bleeping Computer - February 19 2024

In an advisory today Germany's federal intelligence agency (BfV) and South Korea's National Intelligence Service (NIS) warn of an ongoing cyber-espionage operation targeting the global defense sector on behalf of the North Korean government. The attacks aim to steal advanced military technology information and help North Korea modernize conventional arms as well as develop new military capabilities. Today's joint cybersecurity advisory (also available in Korean and German) highlights two cases attributed to North Korean actors, one of them the Lazarus group, to provide the tactics, techniques, and procedures (TTPs) used by the attackers.

[Anatsa Android Trojan Bypasses Google Play Security, Expands Reach to New Countries]

MalwareTips.com - February 19 2024

The Android banking trojan known as Anatsa has expanded its focus to include Slovakia, Slovenia, and Czechia as part of a new campaign observed in November 2023.