Scottish Cyber Coordination Centre

TLP CLEAR: Disclosure is not limited

Daily threat summary

14 December 2023

Vulnerabilities

CISA and Partners Release Advisory on Russian SVR-affiliated Cyber Actors Exploiting CVE-2023-42793

CISA Current Activity - December 13 2023

Today, CISA—along with the U.S. Federal Bureau of Investigation (FBI), National Security Agency (NSA), Polish Military Counterintelligence Service (SKW), CERT Polska (CERT[.]PL), and the UK's National Cyber Security Centre (NCSC)—released a joint Cybersecurity Advisory (CSA), Russian Foreign Intelligence Service (SVR) Exploiting JetBrains TeamCity CVE Globally. Since September 2023, Russian Foreign Intelligence Service (SVR)-affiliated cyber actors (also known as Advanced Persistent Threat 29 (APT 29), the Dukes, CozyBear, and NOBELIUM/Midnight Blizzard) have been targeting servers hosting JetBrains TeamCity software that ultimately enabled them to bypass authorization and conduct arbitrary code execution on the compromised server.

RCE attacks could impact most internet-exposed pfSense instances

SC Magazine US - December 13 2023

More than 92% of internet-exposed instances of the pfSense open-source firewall and router software could be compromised to achieve remote code execution by chaining the reflective XSS vulnerabilities, tracked as CVE-2023-42325 and CVE-2023-42327, as well as the command injection bug, tracked as CVE-2023-42326, all of which have already been addressed by Netgate, according to BleepingComputer.

Hackers are exploiting critical Apache Struts flaw using public PoC

Bleeping Computer - December 13 2023

Hackers are attempting to leverage a recently fixed critical vulnerability (CVE-2023-50164) in Apache Struts that leads to remote code execution, in attacks that rely on publicly available proof-of-concept exploit code. It appears that threat actors have just started, according to the Shadowserver scanning platform, whose researchers observed a small number of IP addresses engaged in exploitation attempts. Apache Struts is an open-source web application framework designed to streamline the development of Java EE web apps, offering a form-based interface and extensive integration capabilities.

TLP CLEAR: Disclosure is not limited

GoTitan Botnet

Red Sky Alliance - X-Industry - RSS - December 13 2023

This past October, Apache issued a critical advisory addressing CVE-2023-46604, a vulnerability involving the deserialization of untrusted data in Apache. On 2 November, the Cybersecurity and Infrastructure Security Agency (CISA) added CVE-2023-46604 to its known exploited list, KEV Catalog, indicating this vulnerability's high risk and impact. Fortiguard Labs also released an outbreak alert and a threat signal report about the active exploitation of CVE-2023-46604, providing more details and recommendations for mitigation.

Malware and threat actors

Lazarus Group Still Deploys Remote Access Trojans

Red Sky Alliance - X-Industry - RSS - December 13 2023

The North Korea-linked threat actor known as the Lazarus Group has been attributed to a new global campaign that involves the opportunistic exploitation of security flaws in Log4j to deploy previously undocumented remote access trojans (RATs) on compromised hosts. Investigators are tracking the activity under the name Operation Blacksmith, noting the use of three DLang-based malware families, including a RAT called NineRAT that leverages Telegram for command-and-control (C2), DLRAT, and a downloader dubbed BottomLoader.

Ukrainian cells and Internet still out, 1 day after suspected Russian cyberattack

ArsTechnica - December 14 2023

Ukrainian civilians on Wednesday grappled for a second day of widespread cellular phone and Internet outages after a cyberattack, purportedly carried out by Kremlin-supported hackers, hit the country’s biggest mobile phone and Internet provider a day earlier. Two separate hacking groups with ties to the Russian government took responsibility for Tuesday’s attack striking Kyivstar, which has said it serves 24.3 million mobile subscribers and more than 1.1 million home Internet users.