Scottish Cyber Coordination Centre

TLP CLEAR: Disclosure is not limited

Daily threat summary

21 March 2024

Vulnerabilities

Critical flaw in Atlassian Bamboo Data Center and Server must be fixed immediately

Security Affairs - March 20 2024

Atlassian fixed tens of vulnerabilities in Bamboo, Bitbucket, Confluence, and Jira products, including a critical flaw that can be very dangerous. Atlassian addressed multiple vulnerabilities in its Bamboo, Bitbucket, Confluence, and Jira products. The most severe vulnerability, tracked as CVE-2024-1597 (CVSS score of 10), is a SQL injection flaw that impacts the org[.]postgresql:postgresql third-party dependency of Bamboo Data Center and Server.

Ivanti Releases Urgent Fix for Critical Sentry RCE Vulnerability

The Hacker News - March 21 2024

Ivanti has disclosed details of a critical remote code execution flaw impacting Standalone Sentry, urging customers to apply the fixes immediately to stay protected against potential cyber threats. Tracked as CVE-2023-41724, the vulnerability carries a CVSS score of 9.6.

Threat actors actively exploit JetBrains TeamCity flaws to deliver malware

Security Affairs - March 20 2024

Multiple threat actors are exploiting the recently disclosed JetBrains TeamCity flaw CVE-2024-27198 in attacks in the wild. Trend Micro researchers are exploiting the recently disclosed vulnerabilities CVE-2024-27198 (CVSS score: 9.8) and CVE-2024-27199 (CVSS score 7.3) security flaws in JetBrains TeamCity to deploy multiple malware families and gain administrative control over impacted systems.

Malware and threat actors

After LockBit, ALPHV Takedowns, RaaS Startups Go on a Recruiting Drive

Dark Reading - March 20 2024

Scottish Cyber Coordination Centre

TLP CLEAR: Disclosure is not limited

Law enforcement action hasn't eradicated ransomware groups, but it has shaken up the cyber underground and sown distrust among thieves.

'Fluffy Wolf' Spreads Meta Stealer in Corporate Phishing Campaign

Dark Reading - March 20 2024

Unsophisticated threat actor is targeting Russian companies with both readily available malware and authentic software.

Five Eyes tell critical infra orgs: take these actions now to protect against China's Volt Typhoon

The Register - Security - March 20 2024

Unless you want to be the next Change Healthcare, that is The Feds and friends yesterday issued yet another warning about China's Volt Typhoon gang, this time urging critical infrastructure owners and operators to protect their facilities against destructive cyber attacks that may be brewing.

New BunnyLoader Malware Variant Surfaces with Modular Attack Features

MalwareTips.com - March 20 2024

Cybersecurity researchers have discovered an updated variant of a stealer and malware loader called BunnyLoader that modularizes its various functions as well as allow it to evade detection.

Open-source ransomware, RATs deployed on compromised TeamCity servers

SC Media - March 20 2024

Jasmin ransomware, SparkRAT and XMRig cryptominers were dropped post-exploitation of CVE-2024-27198.