Scottish Cyber Coordination Centre

TLP CLEAR: Disclosure is not limited

Daily threat summary

30 January 2023

Vulnerabilities

45k Jenkins servers exposed to RCE attacks using public exploits

BleepingComputer.com - January 29 2024

Researchers found roughly 45,000 Jenkins instances exposed online that are vulnerable to CVE-2023-23897, a critical remote code execution (RCE) flaw for which multiple public proof-of-concept (PoC) exploits are in circulation.

Juniper Networks Releases Security Bulletin for J-Web in Junos OS SRX Series and EX Series

CISA Current Activity - January 29 2024

Juniper Networks released a security bulletin to address multiple vulnerabilities for J-Web in Junos OS SRX Series and EX Series. A cyber threat actor could exploit one of these vulnerabilities to take control of an affected system. CISA encourages users and administrators to review the Juniper Bulletin JSA76390 and apply the necessary updates.

Top 10 RCE Vulnerabilities Exploited in 2023

SOCRadar - January 29 2024

Cybersecurity unfolds in a continuous interplay between defenders and threat actors – an ever-evolving quest for software vulnerabilities, with both parties engaged in a strategic game of anticipating each other's next move. One significant category in this landscape is Remote Code Execution (RCE), a subset of Arbitrary Code Execution (ACE) vulnerabilities.

Malware and threat actors

Phobos Ransomware Family Expands With New FAUST Variant

Infosecurity Today - January 29 2024

FortiGuard said the variant was found in an Office document using a VBA script.

Scottish Cyber Coordination Centre

TLP CLEAR: Disclosure is not limited

Trigona Ransomware Threat Actor Uses Mimic Ransomware

ASEC Blog - AhnLab English - January 30 2024

AhnLab SEcurity intelligence Center (ASEC) has recently identified a new activity of the Trigona ransomware threat actor installing Mimic ransomware. Like past cases, the recently detected attack targets MS-SQL servers and is notable for abusing the Bulk Copy Program (BCP) utility in MS-SQL servers during the malware installation process.