Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

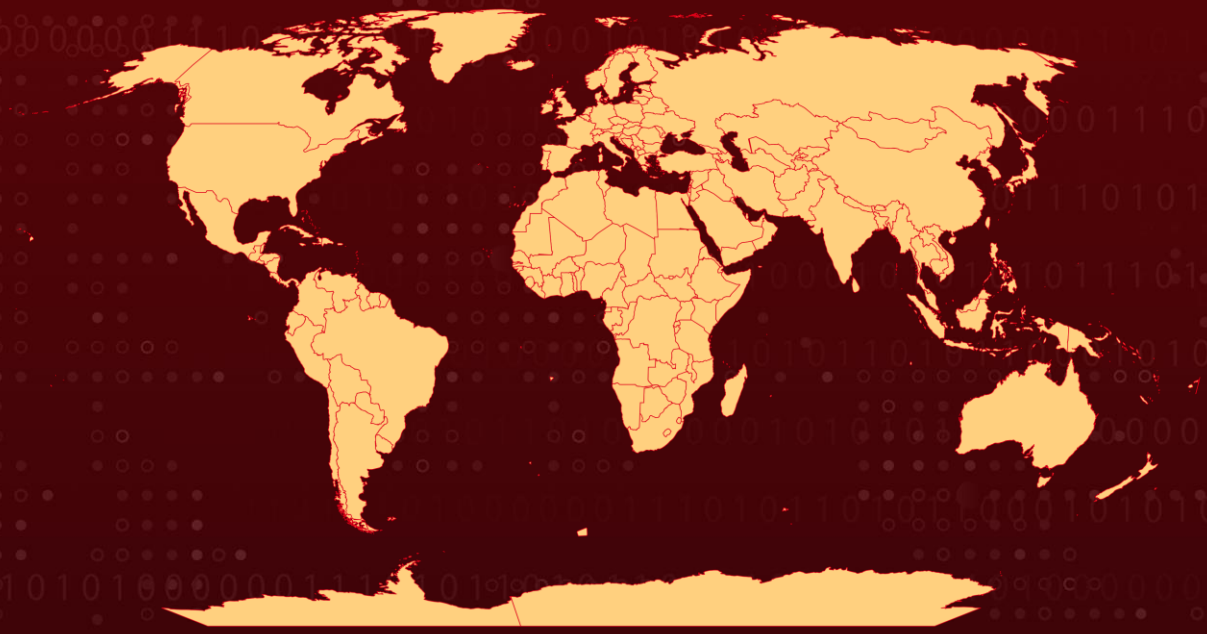
TeamCity Vulnerabilities Unleash Jasmin Ransomware and More

Date of Publication	Admiralty Code	TA Number
March 22, 2024	A1	TA2024113

Summary

Attack Began: January 2024
Malware: Jasmin ransomware, XMRig, SparkRAT backdoor
Attack Region: Worldwide
Attack: Recently patched vulnerabilities in JetBrains TeamCity (CVE-2024-27198, CVE-2024-27199) have emerged as a breeding ground for cyber threats, as attackers leverage them to disseminate various dangers such as Jasmin ransomware, XMRig cryptominers, SparkRAT backdoor, and remote access trojans (RATs). Since the release of proof-of-concept (PoC) code, multiple threat actors have been drawn to these vulnerabilities, using them to execute their malicious intentions.

Attack Regions



CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2024-27198	JetBrains TeamCity Authentication Bypass Vulnerability	TeamCity On-Premises	✗	✓	✓
CVE-2024-27199	JetBrains TeamCity Path Traversal Vulnerability	TeamCity On-Premises	✗	✗	✓

Attack Details

#1 Attackers are exploiting the recently patched JetBrains TeamCity authentication bypass vulnerability (CVE-2024-27198, CVE-2024-27199) to distribute Jasmin ransomware, XMRig cryptominers, SparkRAT backdoor, and remote access trojans (RATs).

#2 Since the emergence of proof-of-concept (PoC) code for both vulnerabilities, multiple threat actors have been identified exploiting them in their malicious activities. This vulnerability allows attackers to steal sensitive data and manipulate a limited range of TeamCity system configurations.

#3 Notably, during the post-exploitation phase, attackers have been observed deploying Jasmin ransomware, which is an open-source tool reminiscent of WannaCry. Some adversaries have chosen to deploy a modified version of the open-source XMRig cryptocurrency mining malware, while others have opted for the open-source Golang-based SparkRAT backdoor.

#4 Jasmin ransomware has the capability to change file extensions to .lsoc and distribute a ransom note named "un-lock your files.html." The attempt to add a user to the local Administrators group is particularly concerning, as it could grant elevated privileges to attackers, aiding in the establishment of a persistent foothold in the system for extended access.

Recommendations

Patch and Update Immediately: Ensure all JetBrains TeamCity installations are promptly patched and updated to mitigate the vulnerabilities (CVE-2024-27198, CVE-2024-27199) that attackers are exploiting.

Robust Backup Strategies: Implement frequent backups for all assets to ensure their complete safety. Implement the 3-2-1-1 backup structure and use specialized tools to provide backup resilience and accessibility.

Network Segmentation: Implement network segmentation to minimize the lateral movement of attackers within the network, limiting their ability to access critical systems and data.

Zero Trust Architecture: Adopt a Zero Trust security architecture, where trust is never assumed and continuous authentication and authorization mechanisms are implemented, reducing the risk of unauthorized access.

Anomaly Detection: Implement anomaly detection algorithms to identify deviations from normal network behavior. This includes monitoring network traffic, system logs, and user activities for any unusual patterns.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0002 Execution	TA0003 Persistence	TA0005 Defense Evasion
TA0007 Discovery	TA0011 Command and Control	TA0010 Exfiltration	TA0040 Impact
T1190 Exploit Public-Facing Application	T1059.001 PowerShell	T1140 Deobfuscate/Decode Files or Information	T1087 Account Discovery
T1482 Domain Trust Discovery	T1105 Ingress Tool Transfer	T1041 Exfiltration Over C2 Channel	T1486 Data Encrypted for Impact

Indicators of Compromise (IOCs)

TYPE	VALUE
URLs	hxxp://207[.]246[.]102[.]242:56641/ABC[.]msi, hxxp://146[.]70[.]149[.]185:58090/JavaAccessBridge-64.msi

TYPE	VALUE
SHA256	56942b36d5990f66a81955a94511298fd27cb6092e467110a7995a0654f17b1a, 32a630decb8fcc8a7ed4811f4293b9d5a242ce7865ab10c19a16fc4aa384bf64, 7cbe0c55b3ca5d12be640e519e4399469399b3eaada20705342fa681befe8c7b, 01db4578f5fb7b29800f7b07a31fda7ff812309f62f7148fca0e246279f6ca61, 908b30abf730a5b51a3d25965eff45a639e881a97505220a38591fe326e00697, 1320e6dd39d9fdb901ae64713594b1153ee6244daa84c2336cf75a2a0b726b3c
IPv4	83[.]97[.]20[.]141, 38[.]54[.]94[.]13

Patch Details

JetBrains has released patches for these vulnerabilities in the latest version 2023.11.4

Link:
https://www.jetbrains.com/teamcity/download/

References

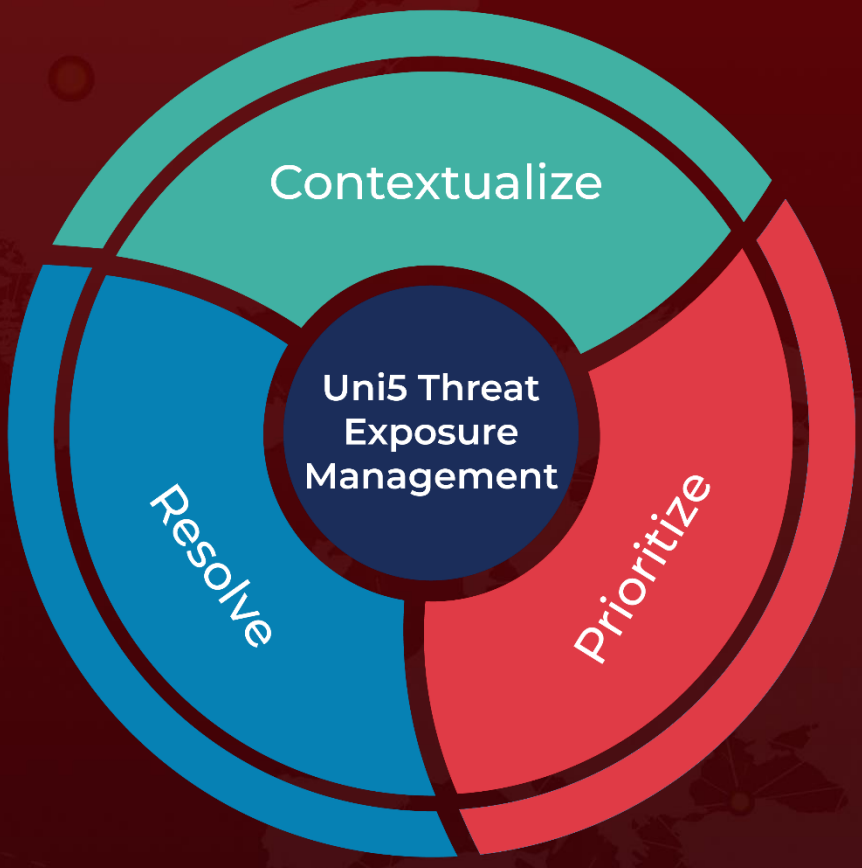
https://www.trendmicro.com/en_us/research/24/c/teamcity-vulnerability-exploits-lead-to-jasmin-ransomware.html

https://www.hivepro.com/threat-advisory/critical-vulnerabilities-discovered-in-teamcity-enable-server-takeover/

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

March 22, 2024 • 5:00 AM

More at www.hivepro.com