Mar 20 2024

NETMANAGEIT

Intelligence Report

TeamCity Vulnerability Exploits Lead to Jasmin Ransomware, Other Malware Types

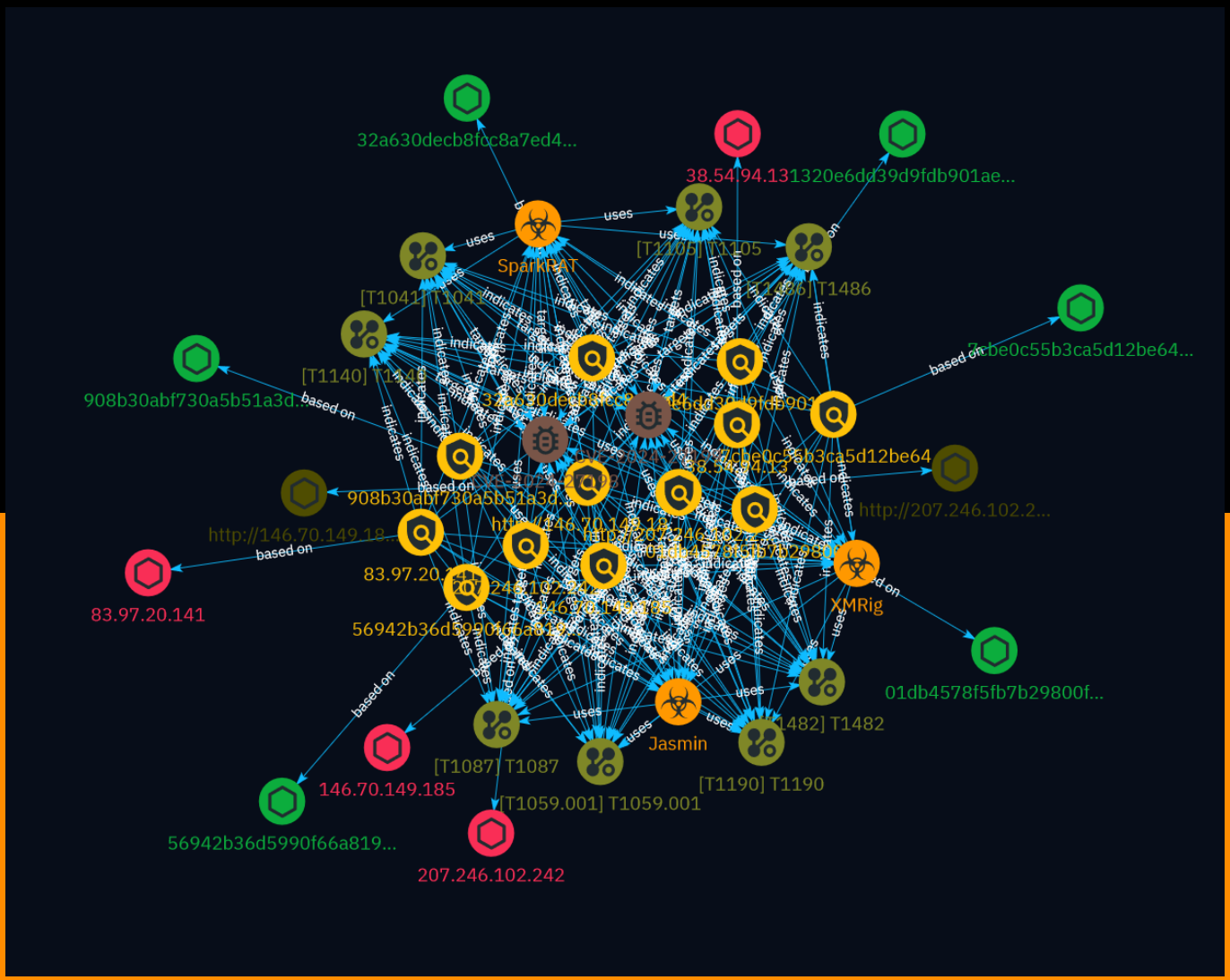

Table of contents

Overview

Entities

Observables

External References

Overview

Description

JetBrains disclosed critical vulnerabilities in TeamCity allowing attackers to bypass authentication and gain control over servers. Actors are exploiting them to deploy ransomware, coinminers and backdoors. Organizations should update affected software immediately.

Confidence

This value represents the confidence in the correctness of the data contained within this report.

100 / 100

Content

N/A

Indicator

Name

1320e6dd39d9fdb901ae64713594b1153ee6244daa84c2336cf75a2a0b726b3c

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '1320e6dd39d9fdb901ae64713594b1153ee6244daa84c2336cf75a2a0b726b3c']

Name

http://207.246.102.242:56641/ABC.msi

Description

- **Unsafe:** False - **Server:** N/A - **Domain Rank:** 0 - **DNS Valid:** False - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': 'N/A', 'timestamp': None, 'iso': None} - **IPQS: Domain:** 207.246.102.242 - **IPQS: IP Address:** N/A

Pattern Type

stix

Pattern

[url:value = 'http://207.246.102.242:56641/ABC.msi']

Name

http://146.70.149.185:58090/JavaAccessBridge-64.msi

Description

- **Unsafe:** False - **Server:** N/A - **Domain Rank:** 0 - **DNS Valid:** False - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': 'N/A', 'timestamp': None, 'iso': None} - **IPQS: Domain:** 146.70.149.185 - **IPQS: IP Address:** N/A

Pattern Type

stix

Pattern

[url:value = 'http://146.70.149.185:58090/JavaAccessBridge-64.msi']

Name

38.54.94.13

Description

- **Zip Code:** N/A - **ISP:** Kaopu Cloud Hk Limited - **ASN:** 138915 - **Organization:** Kaopu Cloud Hk Limited - **Is Crawler:** False - **Timezone:** America/Los_Angeles - **Mobile:** False - **Host:** 38.54.94.13 - **Proxy:** True - **VPN:** True - **TOR:** False - **Active VPN:** False - **Active TOR:** False - **Recent Abuse:** False - **Bot Status:** False - **Connection Type:** Premium required. - **Abuse Velocity:** Premium required. -

Country Code: US - **Region:** California - **City:** San Jose - **Latitude:** 37.18 - **Longitude:** -121.77

Pattern Type

stix

Pattern

[ipv4-addr:value = '38.54.94.13']

Name

908b30abf730a5b51a3d25965eff45a639e881a97505220a38591fe326e00697

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '908b30abf730a5b51a3d25965eff45a639e881a97505220a38591fe326e00697']

Name

7cbe0c55b3ca5d12be640e519e4399469399b3eaada20705342fa681befe8c7b

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '7cbe0c55b3ca5d12be640e519e4399469399b3eaada20705342fa681befe8c7b']

Name

56942b36d5990f66a81955a94511298fd27cb6092e467110a7995a0654f17b1a

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '56942b36d5990f66a81955a94511298fd27cb6092e467110a7995a0654f17b1a']

Name

32a630decb8fcc8a7ed4811f4293b9d5a242ce7865ab10c19a16fc4aa384bf64

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '32a630decb8fcc8a7ed4811f4293b9d5a242ce7865ab10c19a16fc4aa384bf64']

Name

01db4578f5fb7b29800f7b07a31fda7ff812309f62f7148fca0e246279f6ca61

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '01db4578f5fb7b29800f7b07a31fda7ff812309f62f7148fca0e246279f6ca61']

Name

207.246.102.242

Description

- **Zip Code:** N/A - **ISP:** Vultr - **ASN:** 20473 - **Organization:** Vultr - **Is Crawler:** False - **Timezone:** America/Los_Angeles - **Mobile:** False - **Host:** 207.246.102.242.vultrusercontent.com - **Proxy:** True - **VPN:** True - **TOR:** False - **Active VPN:** False - **Active TOR:** False - **Recent Abuse:** False - **Bot Status:** False - **Connection Type:** Premium required. - **Abuse Velocity:** Premium required. - **Country Code:** US - **Region:** California - **City:** Los Angeles - **Latitude:** 34.05 - **Longitude:** -118.24

Pattern Type

stix

Pattern

[ipv4-addr:value = '207.246.102.242']

Name

146.70.149.185

Description

- **Zip Code:** N/A - **ISP:** M247 Europe - **ASN:** 9009 - **Organization:** M247 Europe - **Is Crawler:** False - **Timezone:** Asia/Singapore - **Mobile:** False - **Host:** 146.70.149.185 - **Proxy:** True - **VPN:** True - **TOR:** False - **Active VPN:** True - **Active TOR:** False - **Recent Abuse:** False - **Bot Status:** False - **Connection Type:** Premium required. - **Abuse Velocity:** Premium required. - **Country Code:** SG - **Region:** Singapore - **City:** Singapore - **Latitude:** 1.3 - **Longitude:** 103.78

Pattern Type
stix
Pattern
[ipv4-addr:value = '146.70.149.185']
Name
83.97.20.141
Description
Unknown malware botnet C2 server (confidence level: 75%)
Pattern Type
stix
Pattern
[ipv4-addr:value = '83.97.20.141']

Vulnerability

Name
CVE-2024-27199
Name
CVE-2024-27198
Description
JetBrains TeamCity contains an authentication bypass vulnerability that allows an attacker to perform admin actions.

Malware

Name
Jasmin

Name
XMRig

Name
SparkRAT

Attack-Pattern

Name
T1486
ID
T1486
Description
Adversaries may encrypt data on target systems or on large numbers of systems in a network to interrupt availability to system and network resources. They can attempt to render stored data inaccessible by encrypting files or data on local and remote drives and withholding access to a decryption key. This may be done in order to extract monetary compensation from a victim in exchange for decryption or a decryption key (ransomware) or to render data permanently inaccessible in cases where the key is not saved or transmitted.(Citation: US-CERT Ransomware 2016)(Citation: FireEye WannaCry 2017)(Citation: US-CERT NotPetya 2017)(Citation: US-CERT SamSam 2018) In the case of ransomware, it is typical that common user files like Office documents, PDFs, images, videos, audio, text, and source code files will be encrypted (and often renamed and/or tagged with specific file markers). Adversaries may need to first employ other behaviors, such as [File and Directory Permissions Modification](https://attack.mitre.org/techniques/T1222) or [System Shutdown/Reboot](https://attack.mitre.org/techniques/T1529), in order to unlock and/or gain access to manipulate these files.(Citation: CarbonBlack Conti July 2020) In some cases, adversaries may encrypt critical system files, disk partitions, and the MBR.(Citation: US-CERT NotPetya 2017) To maximize impact on the target organization, malware designed for encrypting data may have worm-like features to propagate across a network by leveraging other attack techniques like [Valid Accounts](https://attack.mitre.org/techniques/T1078), [OS Credential Dumping](https://attack.mitre.org/techniques/T1003), and [SMB/Windows Admin Shares](https://attack.mitre.org/techniques/T1021/002).(Citation: FireEye WannaCry 2017)(Citation: US-CERT NotPetya 2017) Encryption malware may also leverage [Internal

Defacement](https://attack.mitre.org/techniques/T1491/001), such as changing victim wallpapers, or otherwise intimidate victims by sending ransom notes or other messages to connected printers (known as "print bombing").(Citation: NHS Digital Egregor Nov 2020) In cloud environments, storage objects within compromised accounts may also be encrypted. (Citation: Rhino S3 Ransomware Part 1)

Name

T1059.001

ID

T1059.001

Description

Adversaries may abuse PowerShell commands and scripts for execution. PowerShell is a powerful interactive command-line interface and scripting environment included in the Windows operating system.(Citation: TechNet PowerShell) Adversaries can use PowerShell to perform a number of actions, including discovery of information and execution of code. Examples include the `Start-Process` cmdlet which can be used to run an executable and the `Invoke-Command` cmdlet which runs a command locally or on a remote computer (though administrator permissions are required to use PowerShell to connect to remote systems). PowerShell may also be used to download and run executables from the Internet, which can be executed from disk or in memory without touching disk. A number of PowerShell-based offensive testing tools are available, including [Empire](https://attack.mitre.org/software/S0363), [PowerSploit](https://attack.mitre.org/software/S0194), [PoshC2](https://attack.mitre.org/software/S0378), and PSAttack.(Citation: Github PSAttack) PowerShell commands/scripts can also be executed without directly invoking the `powershell.exe` binary through interfaces to PowerShell's underlying `System.Management.Automation` assembly DLL exposed through the .NET framework and Windows Common Language Interface (CLI).(Citation: Sixdub PowerPick Jan 2016)(Citation: SilentBreak Offensive PS Dec 2015)(Citation: Microsoft PSfromCsharp APR 2014)

Name

T1041

ID

T1041

Description

Adversaries may steal data by exfiltrating it over an existing command and control channel. Stolen data is encoded into the normal communications channel using the same protocol as command and control communications.

Name

T1482

ID

T1482

Description

Adversaries may attempt to gather information on domain trust relationships that may be used to identify lateral movement opportunities in Windows multi-domain/forest environments. Domain trusts provide a mechanism for a domain to allow access to resources based on the authentication procedures of another domain.(Citation: Microsoft Trusts) Domain trusts allow the users of the trusted domain to access resources in the trusting domain. The information discovered may help the adversary conduct [SID-History Injection](https://attack.mitre.org/techniques/T1134/005), [Pass the Ticket](https://attack.mitre.org/techniques/T1550/003), and [Kerberoasting](https://attack.mitre.org/techniques/T1558/003).(Citation: AdSecurity Forging Trust Tickets)(Citation: Harmj0y Domain Trusts) Domain trusts can be enumerated using the `DSEnumerateDomainTrusts()` Win32 API call, .NET methods, and LDAP.(Citation: Harmj0y Domain Trusts) The Windows utility [Nltest](https://attack.mitre.org/software/S0359) is known to be used by adversaries to enumerate domain trusts.(Citation: Microsoft Operation Wilysupply)

Name

T1087

ID

T1087

Description

Adversaries may attempt to get a listing of valid accounts, usernames, or email addresses on a system or within a compromised environment. This information can help adversaries determine which accounts exist, which can aid in follow-on behavior such as brute-forcing, spear-phishing attacks, or account takeovers (e.g., [Valid Accounts](https://attack.mitre.org/techniques/T1078)). Adversaries may use several methods to enumerate accounts, including abuse of existing tools, built-in commands, and potential misconfigurations that leak account names and roles or permissions in the targeted environment. For examples, cloud environments typically provide easily accessible interfaces to obtain user lists. On hosts, adversaries can use default [PowerShell](https://attack.mitre.org/techniques/T1059/001) and other command line functionality to identify accounts. Information about email addresses and accounts may also be extracted by searching an infected system's files.

Name

T1105

ID

T1105

Description

Adversaries may transfer tools or other files from an external system into a compromised environment. Tools or files may be copied from an external adversary-controlled system to the victim network through the command and control channel or through alternate protocols such as [ftp](https://attack.mitre.org/software/S0095). Once present, adversaries may also transfer/spread tools between victim devices within a compromised environment (i.e. [Lateral Tool Transfer](https://attack.mitre.org/techniques/T1570)). On Windows, adversaries may use various utilities to download tools, such as `copy`, `finger`, [certutil](https://attack.mitre.org/software/S0160), and [PowerShell](https://attack.mitre.org/techniques/T1059/001) commands such as `IEX(New-Object Net.WebClient).downloadString()` and `Invoke-WebRequest`. On Linux and macOS systems, a variety of utilities also exist, such as `curl`, `scp`, `sftp`, `tftp`, `rsync`, `finger`, and `wget`. (Citation: t1105_lolbas) Adversaries may also abuse installers and package managers, such

as `yum` or `winget`, to download tools to victim hosts. Files can also be transferred using various [Web Service](https://attack.mitre.org/techniques/T1102)s as well as native or otherwise present tools on the victim system.(Citation: PTSecurity Cobalt Dec 2016) In some cases, adversaries may be able to leverage services that sync between a web-based and an on-premises client, such as Dropbox or OneDrive, to transfer files onto victim systems. For example, by compromising a cloud account and logging into the service's web portal, an adversary may be able to trigger an automatic syncing process that transfers the file onto the victim's machine.(Citation: Dropbox Malware Sync)

Name

T1190

ID

T1190

Description

Adversaries may attempt to exploit a weakness in an Internet-facing host or system to initially access a network. The weakness in the system can be a software bug, a temporary glitch, or a misconfiguration. Exploited applications are often websites/web servers, but can also include databases (like SQL), standard services (like SMB or SSH), network device administration and management protocols (like SNMP and Smart Install), and any other system with Internet accessible open sockets.(Citation: NVD CVE-2016-6662)(Citation: CIS Multiple SMB Vulnerabilities)(Citation: US-CERT TA18-106A Network Infrastructure Devices 2018)(Citation: Cisco Blog Legacy Device Attacks)(Citation: NVD CVE-2014-7169) Depending on the flaw being exploited this may also involve [Exploitation for Defense Evasion](https://attack.mitre.org/techniques/T1211). If an application is hosted on cloud-based infrastructure and/or is containerized, then exploiting it may lead to compromise of the underlying instance or container. This can allow an adversary a path to access the cloud or container APIs, exploit container host access via [Escape to Host](https://attack.mitre.org/techniques/T1611), or take advantage of weak identity and access management policies. Adversaries may also exploit edge network infrastructure and related appliances, specifically targeting devices that do not support robust host-based defenses.(Citation: Mandiant Fortinet Zero Day)(Citation: Wired Russia Cyberwar) For websites and databases, the OWASP top 10 and CWE top 25 highlight the most common web-based vulnerabilities. (Citation: OWASP Top 10)(Citation: CWE top 25)

Name

T1140

ID

T1140

Description

Adversaries may use [Obfuscated Files or Information](https://attack.mitre.org/techniques/T1027) to hide artifacts of an intrusion from analysis. They may require separate mechanisms to decode or deobfuscate that information depending on how they intend to use it. Methods for doing that include built-in functionality of malware or by using utilities present on the system. One such example is the use of [certutil](https://attack.mitre.org/software/S0160) to decode a remote access tool portable executable file that has been hidden inside a certificate file.(Citation: Malwarebytes Targeted Attack against Saudi Arabia) Another example is using the Windows `copy /b` command to reassemble binary fragments into a malicious payload.(Citation: Carbon Black Obfuscation Sept 2016) Sometimes a user's action may be required to open it for deobfuscation or decryption as part of [User Execution](https://attack.mitre.org/techniques/T1204). The user may also be required to input a password to open a password protected compressed/encrypted file that was provided by the adversary. (Citation: Volexity PowerDuke November 2016)

StixFile

Value
1320e6dd39d9fdb901ae64713594b1153ee6244daa84c2336cf75a2a0b726b3c
908b30abf730a5b51a3d25965eff45a639e881a97505220a38591fe326e00697
7cbe0c55b3ca5d12be640e519e4399469399b3eaada20705342fa681befe8c7b
56942b36d5990f66a81955a94511298fd27cb6092e467110a7995a0654f17b1a
32a630decb8fcc8a7ed4811f4293b9d5a242ce7865ab10c19a16fc4aa384bf64
01db4578f5fb7b29800f7b07a31fda7ff812309f62f7148fca0e246279f6ca61

Url

Value
http://207.246.102.242:56641/ABC.msi
http://146.70.149.185:58090/JavaAccessBridge-64.msi

IPv4-Addr

Value
38.54.94.13
207.246.102.242
146.70.149.185
83.97.20.141

External References

- https://www.trendmicro.com/content/dam/trendmicro/global/en/research/24/c/teamcity-vulnerability-exploits-lead-to-jasmin-ransomware/ioc-teamcity.txt
- https://www.trendmicro.com/en_us/research/24/c/teamcity-vulnerability-exploits-lead-to-jasmin-ransomware.html
- https://otx.alienvault.com/pulse/65fab288320597ab71eabfa8