Hive Pro®

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

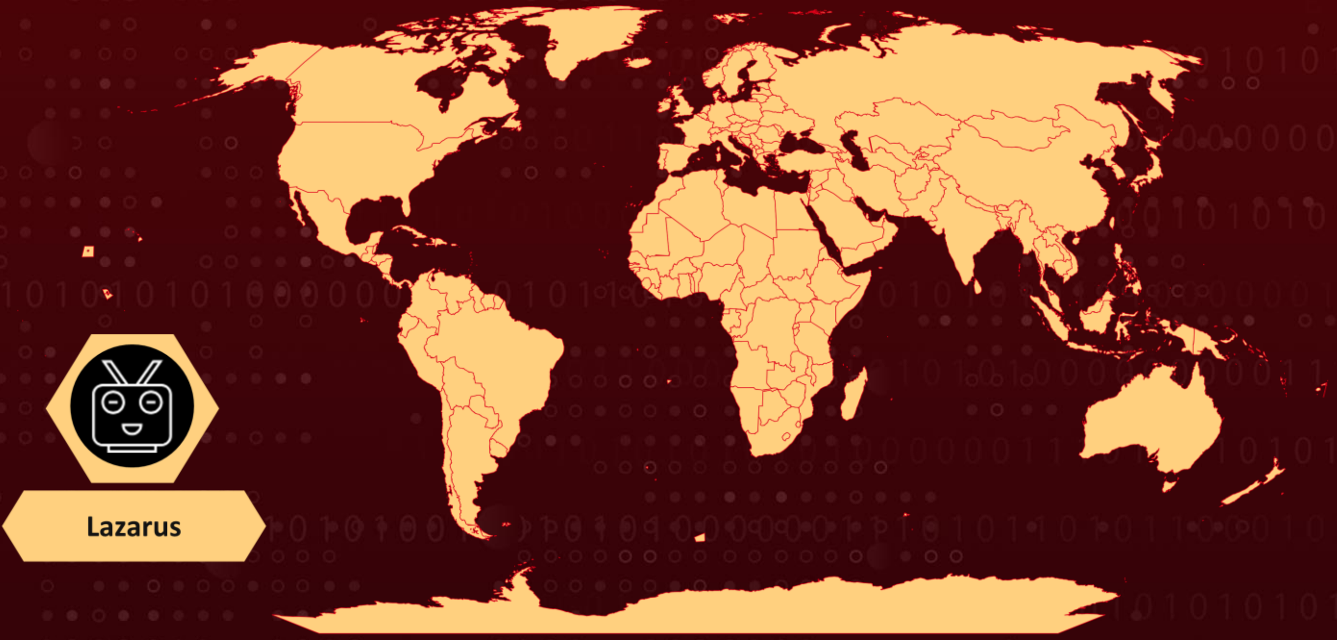
North Korean Actors Behind Active Exploitation of TeamCity Vulnerability

Date of Publication	Admiralty Code	TA Number
October 19, 2023	A1	TA2023425

Summary

Attack Began: Early October 2023
Attack Region: Worldwide
Actor: Lazarus Group (aka Labyrinth Chollima, Guardians Of Peace, Zinc, Nickel Academy, Group 77, Hastati Group, Whois Hacking Team, Newromanic Cyber Army Team, Hidden Cobra, Appleworm, APT-C-26, Atk 3, Sectora01, ITG03, TA404, DEV-0139, Gods Apostles, Gods Disciples, UNC577, UNC2970, UNC4034, UNC4736, UNC4899, Diamond Sleet, Jade Sleet, TraderTraitor) and Andariel (aka Silent Chollima, Stonefly, Plutonium, Onyx Sleet)
Malware: ForestTiger, FeedLoad, RollSling, HazyLoad
Attack: The North Korean threat actors Lazarus and its subgroup Andariel are actively exploiting the CVE-2023-42793 vulnerability, which is an authentication bypass vulnerability, after successful exploitation, an attacker can perform a remote code execution attack and gain administrative control of the TeamCity server. These groups are deploying backdoor through this vulnerability, and their activities are likely aimed at conducting software supply chain attacks.

Attack Regions



Powered by Bing
© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, Open Places, OpenStreetMap, TomTom, Zenrin

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH
CVE-2023-42793	JetBrains TeamCity Authentication Bypass Vulnerability	TeamCity	✗	✓	✓

Attack Details

#1 The North Korean hacking groups Lazarus and Andariel, with Andariel a subgroup of Lazarus, are actively exploiting the CVE-2023-42793 vulnerability in TeamCity servers. This vulnerability allows for remote code execution and affects multiple versions of JetBrains TeamCity, which is a popular continuous integration and deployment server used by organizations for software deployment. Their purpose for this exploitation is to deploy backdoor.

#2 While both Lazarus and Andariel are currently exploiting the CVE-2023-42793 vulnerability in TeamCity servers, it is observed that they employ different sets of tools and malwares once they successfully exploit the vulnerability. After successfully breaching the TeamCity server, the threat actors employ multiple attack chains to establish backdoors.

#3 In the first attack chain, Lazarus deploys the ForestTiger malware, which serves as a backdoor, granting the threat actors the ability to execute commands on the compromised server. In the second attack chain, the actors utilize DLL search order hijacking attacks to initiate a malware loader known as FeedLoad. This loader's primary function is to install a RAT, providing the threat actors with remote control and access to the affected server. Following a successful compromise, Lazarus is extracting credentials from the LSASS memory.

#4 Andariel takes a more direct approach in their attacks by creating a 'krtbgt' admin account on the breached TeamCity server and then run commands to collect system information. These threat actors subsequently deploy a payload that installs the HazyLoad proxy tool, facilitating a persistent connection between the compromised server and Andariel's servers. Regardless of the specific techniques used, the attackers ultimately extract credentials from the LSASS memory. Observing the actor’s past operations, they can potentially conduct software supply chain attacks possessing a particularly high risk to organizations who are affected.

Recommendations

Apply Patch: Install the security patch provided by TeamCity to address the CVE-2023-42793 vulnerability. This patch closes the security gap that allows attackers to exploit the vulnerability.

Robust Endpoint Security: Deploy advanced endpoint security solutions that include real-time malware detection and behavioral analysis. Regularly update antivirus and anti-malware software to ensure the latest threat definitions are in place. A multi-layered approach to endpoint security can prevent malwares from infiltrating the network through vulnerable endpoints and can detect and block malicious activities effectively.

Monitor User Accounts: Utilize automated systems for System Event Monitoring, ensuring constant surveillance of account creation activities in real time. The monitoring platform should be capable of instantly notifying administrators or security teams upon detecting any suspicious activities.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	**TA0002** Execution	**TA0004** Privilege Escalation	**TA0011** Command and Control
TA0003 Persistence	**TA0006** Credential Access	**TA0008** Lateral Movement	**TA0007** Discovery
T1588 Obtain Capabilities	**T1588.006** Vulnerabilities	**T1059** Command and Scripting Interpreter	**T1059.001** PowerShell
T1574 Hijack Execution Flow	**T1574.001** DLL Search Order Hijacking	**T1105** Ingress Tool Transfer	**T1136** Create Account
T1021 Remote Services	**T1021.001** Remote Desktop Protocol	**T1003** OS Credential Dumping	**T1003.001** LSASS Memory
T1007 System Service Discovery			

Indicators of Compromise (IOCs)

TYPE	VALUE
URLs	hxxp://www.bandarpowder[.]com/public/assets/img/cfg.png, hxxps://www.bandarpowder[.]com/public/assets/img/cfg.png, hxxp://www.aeon-petro[.]com/wcms/plugins/addition_contents/cfg.png, hxxp://www.bandarpowder[.]com/public/assets/img/user64.png, hxxps://www.bandarpowder[.]com/public/assets/img/user64.png, hxxp://www.aeon-petro[.]com/wcms/plugins/addition_contents/user64.png, hxxp://www.mge[.]sn/themes/classic/modules/ps_rssfeed/feed.zip, hxxp://www.mge[.]sn/themes/classic/modules/ps_rssfeed/feedmd.zip, hxxps://vadtalmandir[.]org/admin/ckeditor/plugins/icontact/about.php, hxxps://commune-fraita[.]ma/wp-content/plugins/wp-contact/contact.php, hxxp://147.78.149[.]201:9090/imgr.ico, hxxp://162.19.71[.]175:7443/bottom.gif
SHA256	e06f29dccfe90ae80812c2357171b5c48fba189ae103d28e972067b107e58795, 0be1908566efb9d23a98797884f2827de040e4cedb642b60ed66e208715ed4aa, d9add2bfdfebfa235575687de356f0cefb3e4c55964c4cb8bfdcdc58294eeaca, f251144f7ad0be0045034a1fc33fb896e8c32874e0b05869ff5783e14c062486, fa7f6ac04ec118dd807c1377599f9d369096c6d8fb1ed24ac7a6ec0e817eaab6, 000752074544950ae9020a35ccd77de277f1cd5026b4b9559279dc3b86965eee
Filepath	C:\ProgramData\Forest64.exe, C:\ProgramData\4800-84DC-063A6A41C5C, C:\ProgramData\DSROLE.dll, C:\ProgramData\Version.dll, C:\ProgramData\readme.md, C:\ProgramData\wsmprovhost.exe, C:\ProgramData\clip.exe, C:\Windows\Temp\temp.exe, C:\Windows\ADFS\bg\inetmgr.exe
Domains	dersmarketim[.]com, olidhealth[.]com, galerielamy[.]com, 3dkit[.]org

Patch Link

Update your server to the latest version 2023.05.4
Link:
https://www.jetbrains.com/teamcity/download/other.html

If update of TeamCity server to the latest version is not feasible, apply the fixed plugins provided by JetBrains.

Link for Versions prior to 2018.1:
https://download.jetbrains.com/teamcity/plugins/internal/CVE-2023-42793-fix-2018-1.zip

Link for Versions 2018.2+ :
https://download.jetbrains.com/teamcity/plugins/internal/CVE-2023-42793-fix-recent-versions.zip

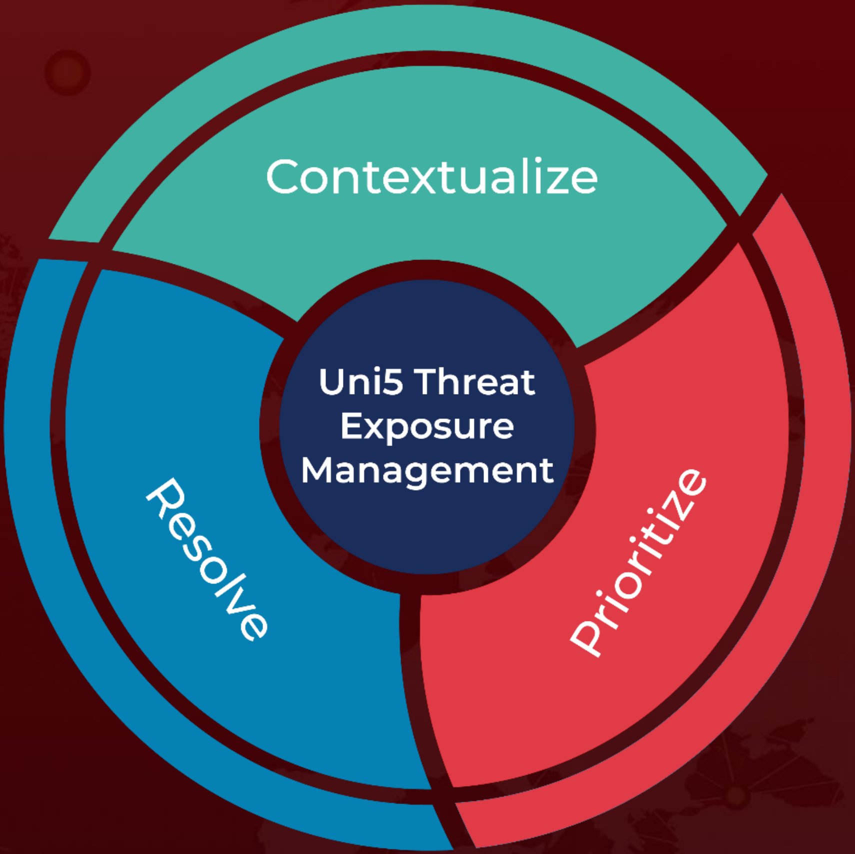
References

https://www.microsoft.com/en-us/security/blog/2023/10/18/multiple-north-korean-threat-actors-exploiting-the-teamcity-cve-2023-42793-vulnerability/

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

October 19, 2023 • 6:00 AM

More at www.hivepro.com