Hive Pro®

Threat Level

Red

CISA: AA23-347A

HiveForce Labs

# THREAT ADVISORY

## ATTACK REPORT

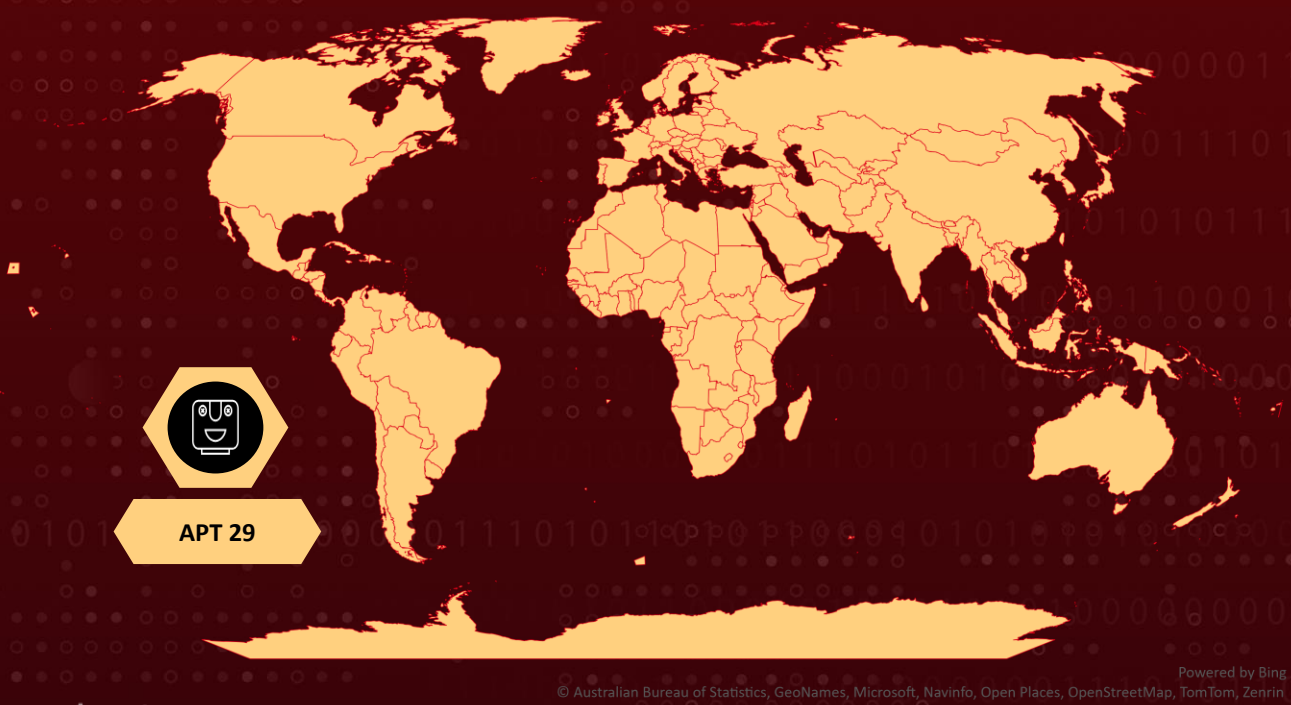
# Russian SVR Exploits Critical TeamCity Vulnerability Globally

| Date of Publication | Admiralty Code | TA Number |
| --- | --- | --- |
| December 14, 2023 | A1 | TA2023505 |

# Summary

**Attack Began:** September 2023
**Attack Region:** Worldwide
**Threat Actor:** APT 29 (aka Midnight Blizzard, Cozy Bear, The Dukes, Group 100, Yttrium, Iron Hemlock, Minidionis, CloudLook, ATK 7, ITG11, Grizzly Steppe, UNC2452, Dark Halo, SolarStorm, StellarParticle, SilverFish, Nobelium, Iron Ritual, Cloaked Ursa, BlueBravo)
**Targeted Industries:** Government, Political, Diplomatic agencies, and Technology
**Affected Products:** JetBrains TeamCity versions prior to 2023.05.4
**Malware:** GraphicalProton
**Attack:** A critical vulnerability (CVE-2023-45247) in JetBrains TeamCity is actively exploited by Russia's SVR cyber actors (APT 29), allowing full server compromise. The targeted software widely used by developers poses a significant threat, enabling access to sensitive information and potential manipulation of software development processes.

## Attack Regions




## CVE

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

# Attack Details

**#1**

A critical vulnerability (CVE-2023-45247) in JetBrains TeamCity is actively exploited by the Russian Foreign Intelligence Service (SVR) cyber actors named APT 29 group (aka CozyBear, NOBELIUM/Midnight Blizzard). The vulnerability allows attackers to inject malicious code into server-side templates used by TeamCity, leading to complete server compromise with administrator privileges. TeamCity is widely used by developers for managing software compilation, building, testing, and releasing.

**#2**

If successfully compromised, the TeamCity servers provide attackers with access to sensitive information, including source code, signing certificates, and the ability to manipulate software development processes. While the SVR has not replicated the widespread impact of its 2020 SolarWinds attack, it has been observed using the TeamCity vulnerability to escalate privileges, move laterally, deploy additional backdoors, and ensure long-term access to compromised networks.

**#3**

The SVR's operation involves exploiting TeamCity servers, conducting host reconnaissance, exfiltrating sensitive files, avoiding detection through various techniques such as disabling antivirus software, and using covert communication channels. The SVR's toolset includes custom and open-source tools like GraphicalProton, which uses cloud services for communication. There's also an HTTPS variant introduced by the SVR that relies on HTTP requests and a re-registered expired domain with a dummy WordPress website for command and control (C2) communication.

**#4**

Researchers are tracking almost 800 unpatched TeamCity servers vulnerable to attacks. North Korean state-backed groups, Lazarus and Andariel, were found using CVE-2023-42793 exploits to backdoor victims' networks, potentially preparing for software supply chain attacks.

# Recommendations

**Apply Security Patches:** Apply the security patches for CVE-2023-42793 released by JetBrains TeamCity in mid-September 2023. Ensure that all systems are promptly updated to mitigate the known vulnerability.

**Network Monitoring:** Monitor the network for evidence of encoded commands and the execution of network scanning tools. Detecting unusual network activity can help identify potential threats early.

**Enhance Monitoring and Detection:** Strengthen monitoring capabilities to detect unusual or unauthorized activities on TeamCity servers. Utilize intrusion detection systems and anomaly detection mechanisms to identify potential threats.

**Multi-Factor Authentication (MFA):** Require the use of multi-factor authentication (MFA) for all services, especially for email, virtual private networks, and accounts with access to critical systems. MFA enhances security by requiring multiple verification methods.

## Potential MITRE ATT&CK TTPs

| | | | |
|---|---|---|---|
| TA0001<br>Initial Access | TA0002<br>Execution | TA0009<br>Collection | TA0006<br>Credential Access |
| TA0043<br>Reconnaissance | TA0003<br>Persistence | TA0004<br>Privilege Escalation | TA0005<br>Defense Evasion |
| TA0007<br>Discovery | TA0008<br>Lateral Movement | TA0011<br>Command and Control | TA0010<br>Exfiltration |
| T1590.004<br>Network Topology | T1590<br>Gather Victim Network Information | T1592.002<br>Software | T1592<br>Gather Victim Host Information |
| T1190<br>Exploit Public-Facing Application | T1059.001<br>PowerShell | T1059<br>Command and Scripting Interpreter | T1059.003<br>Windows Command Shell |
| T1203<br>Exploitation for Client Execution | T1574.002<br>DLL Side-Loading | T1574<br>Hijack Execution Flow | T1053.005<br>Scheduled Task |

| | | | |
|---|---|---|---|
| T1053<br>Scheduled Task/Job | T1505.001<br>SQL Stored Procedures | T1505<br>Server Software Component | T1547<br>Boot or Logon Autostart Execution |
| T1068<br>Exploitation for Privilege Escalation | T1098<br>Account Manipulation | T1027.001<br>Binary Padding | T1027<br>Obfuscated Files or Information |
| T1036<br>Masquerading | T1055<br>Process Injection | T1562.001<br>Disable or Modify Tools | T1562<br>Impair Defenses |
| T1564<br>Hide Artifacts | T1564.001<br>Hidden Files and Directories | T1003.001<br>LSASS Memory | T1003.002<br>Security Account Manager |
| T1555.003<br>Credentials from Web Browsers | T1558.001<br>Golden Ticket | T1033<br>System Owner/User Discovery | T1046<br>Network Service Discovery |
| T1057<br>Process Discovery | T1567<br>Exfiltration Over Web Service | T1210<br>Exploitation of Remote Services | T1047<br>Windows Management Instrumentation |
| T1568<br>Dynamic Resolution | T1572<br>Protocol Tunneling | T1020<br>Automated Exfiltration | T1041<br>Exfiltration Over C2 Channel |

## Indicators of Compromise (IOCs)

| TYPE | VALUE |
|---|---|
| MD5 | 2d8e4f38b36c334d0a32a7324832501d,<br>c996d7971c49252c582171d9380360f2, |
| SHA1 | c948ae14761095e4d76b55d9de86412258be7afd,<br>f6f11ad2cd2b0cf95ed42324876bee1d83e01775, |
| IPv4 | 103[.]76[.]128[.]34,<br>65[.]21[.]51[.]58,<br>65[.]20[.]97[.]203 |

| TYPE | VALUE |
| --- | --- |
| Domains | matclick[.]com,<br>poetpages[.]com, |
| SHA256 | 01aa278b07b58dc46c84bd0b1b5c8e9ee4e62ea0bf7a695862444af32e87f1fd,<br>01b5f7094de0b2c6f8e28aa9a2ded678c166d615530e595621e692a9c0240732,<br>0296e2ce999e67c76352613a718e11516fe1b0efc3ffdb8918fc999dd76a73a5,<br>18101518eae3eec6ebe453de4c4c380160774d7c3ed5c79e1813013ac1bb0b93,<br>19f1ef66e449cf2a2b0283dbb756850cca396114286e1485e35e6c672c9c3641,<br>1e74cf0223d57fd846e171f4a58790280d4593df1f23132044076560a5455ff8,<br>219fb90d2e88a2197a9e08b0e7811e2e0bd23d59233287587ccc4642c2cf3d67,<br>34c8f155601a3948ddb0d60b582cfe87de970d443cc0e05df48b1a1ad2e42b5e,<br>4bf1915785d7c6e0987eb9c15857f7ac67dc365177a1707b14822131d43a6166,<br>4ee70128c70d646c5c2a9a17ad05949cb1fbf1043e9d671998812b2dce75cf0f,<br>620d2bf14fe345eef618fdd1dac242b3a0bb65ccb75699fe00f7c671f2c1d869,<br>773f0102720af2957859d6930cd09693824d87db705b3303cef9ee794375ce13,<br>7b666b978dbbe7c032cef19a90993e8e4922b743ee839632bfa6d99314ea6c53,<br>8afb71b7ce511b0bce642f46d6fc5dd79fad86a58223061b684313966efef9c7,<br>92c7693e82a90d08249edeafbca6533fed81b62e9e056dec34c24756e0a130a6,<br>950adbaf66ab214de837e6f1c00921c501746616a882ea8c42f1bad5f9b6eff4,<br>971f0ced6c42dd2b6e3ea3e6c54d0081cf9b06e79a38c2ede3a2c5228c27a6dc,<br>b53e27c79eed8531b1e05827ace2362603fb9f77f53cee2e34940d570217cbf7,<br>c37c109171f32456bbe57b8676cc533091e387e6ba733fbaa01175c43cfb6ebd,<br>c40a8006a7b1f10b1b42fdd8d6d0f434be503fb3400fb948ac9ab8ddfa5b78a0,<br>c7b01242d2e15c3da0f45b8adec4e6913e534849cde16a2a6c480045e03fbee4,<br>c832462c15c8041191f190f7a88d25089d57f78e97161c3003d68d0cc2c4baa3,<br>cb83e5cb264161c28de76a44d0edb450745e773d24bec5869d85f69633e44dcf, |

| TYPE | VALUE |
| --- | --- |
| SHA256 | cd3584d61c2724f927553770924149bb51811742a461146b15b34a26c92cad43, d724728344fcf3812a0664a80270f7b4980b82342449a8c5a2fa510e10600443, ebe231c90fad02590fc56d5840acc63b90312b0e2fee7da3c7606027ed92600e, f1b40e6e5a7cbc22f7a0bd34607b13e7e3493b8aad7431c47f1366f0256e23eb, f6194121e1540c3553273709127dfa1daab96b0acfab6e92548bfb4059913c69 |
| URL | https://matclick[.]com/wp-query[.]php |

## Patch Details

Update your server to the either patch version 2023.05.4 or to the latest version available.

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.cisa.gov/news-events/cybersecurity-advisories/aa23-347a

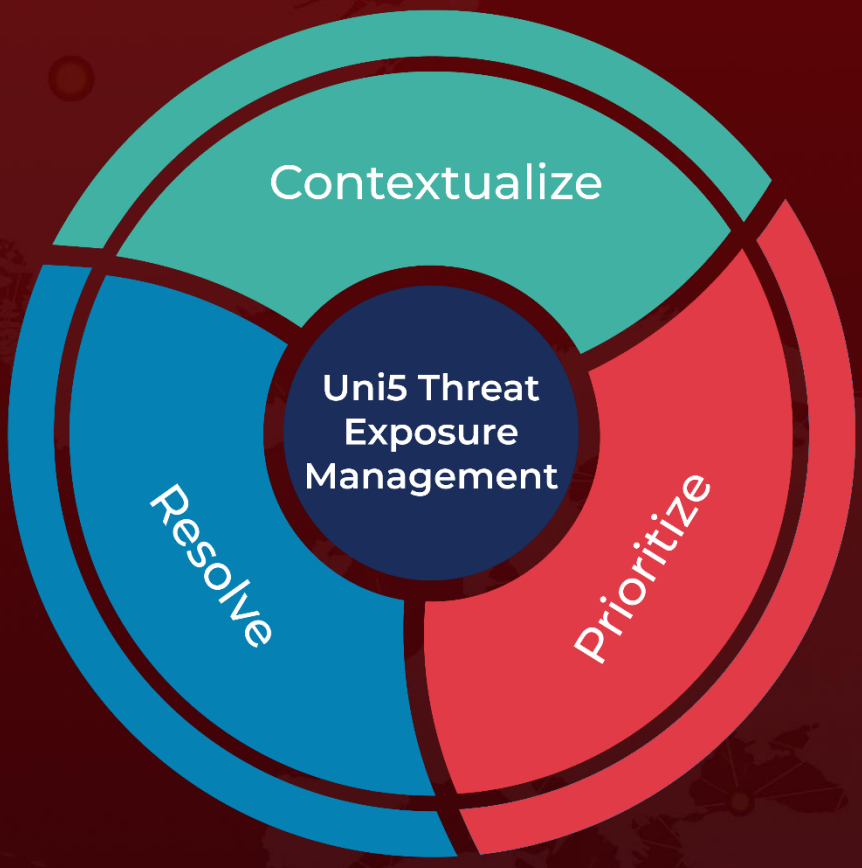
https://www.hivepro.com/threat-advisory/north-korean-actors-behind-active-exploitation-of-teamcity-vulnerability/

https://www.hivepro.com/threat-advisory/new-apt-29-campaign-targets-organizations-through-microsoft-teams/

# 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

**December 14, 2023 . 4:00 AM**

© 2023 All Rights are Reserved by Hive Pro®

More at www.hivepro.com