FORTINET

OUTBREAK ALERTS

JetBrains TeamCity Authentication Bypass Attack

Advanced Persistent Threat Groups exploiting the flaw in (CI/CD) application

https://www.fortinet.com/blog/threat-research/teamcity-intrusion-saga-apt29-suspected-exploiting-cve-2023-42793
CVEs: CVE-2023-42793

Multiple Threat actors seen exploiting the authentication bypass flaw in JetBrains TeamCity that could lead to remote code execution. If compromised, they can access a TeamCity server, gaining entry to a software developer's source code, signing certificates, and the power to manipulate software building and deployment procedures. This access could also be misused by these malicious actors to carry out supply chain operations.

Background

TeamCity is a continuous integration/continuous deployment (CI/CD) application used by organizations for DevOps and other software development activities. Software developers use TeamCity software to manage and automate software compilation, building, testing, and releasing.

Announced

September 6, 2023: Researchers from Sonar discovered a critical TeamCity On-Premises vulnerability (CVE-2023-42793).

September 20, 2023: JetBrains released the advisory and hot fixes for the vulnerability.
https://blog.jetbrains.com/teamcity/2023/09/critical-security-issue-affecting-teamcity-on-premises-update-to-2023-05-4-now/

September 27, 2023: A public exploit for this vulnerability was released by Rapid7.

In mid-October 2023, the FortiGuard Incident Response (IR) team was engaged to investigate a compromised organization's network. See full details on the blog.
https://www.fortinet.com/blog/threat-research/teamcity-intrusion-saga-apt29-suspected-exploiting-cve-2023-42793

Oct 18, 2023: Microsoft Threat Intelligence reported that multiple North Korean threat actors exploiting the TeamCity CVE-2023-42793 vulnerability
https://www.microsoft.com/en-us/security/blog/2023/10/18/multiple-north-korean-threat-actors-exploiting-the-teamcity-cve-2023-42793-vulnerability/

Latest Developments

December 13, 2023: FortiGuard Labs released a detailed threat research on a different threat actor, (APT-29) exploiting CVE-2023-42793
https://www.fortinet.com/blog/threat-research/teamcity-intrusion-saga-apt29-suspected-exploiting-cve-2023-42793

December 13, 2023: CISA and Partners Release Advisory on Russian SVR-affiliated Cyber Actors Exploiting CVE-2023-42793
https://www.cisa.gov/news-events/alerts/2023/12/13/cisa-and-partners-release-advisory-russian-svr-affiliated-cyber-actors-exploiting-cve-2023-42793

According to CISA's advisory, as a result of this latest SVR cyber activity, they identified a few dozen compromised companies in the United States, Europe, Asia, and Australia and the identified victims included: an energy trade association; companies that provide software for billing, medical devices, customer care, employee monitoring, financial management, marketing, sales, and video games; as well as hosting companies, tools manufacturers, and small and large IT companies.

PROTECT

Countermeasures across the security fabric for protecting assets, data and network from cybersecurity events:

- Reconnaissance
- Weaponization
- Delivery

AV

Detects and blocks malware related to JetBrains TeamCity Authentication Bypass Attack (CVE-2023-42793)

FortiGate *DB 91.09703*
FortiWeb *DB 91.09703*
FortiClient *DB 91.09703*
FortiSASE *DB 91.09703*
FortiMail *DB 91.09703*
FortiCASB *DB 91.09703*
FortiCWP *DB 91.09703*
FortiADC *DB 91.09703*
FortiProxy *DB 91.09703*

Vulnerability

Detects vulnerable JetBrains TeamCity application running on the network

FortiClient *DB 1.545*

AV (Pre-filter)

Detects and blocks malware related to JetBrains TeamCity Authentication Bypass Attack (CVE-2023-42793)

FortiEDR *DB 91.09703*
FortiSandbox *DB 91.09703*
FortiNDR *DB 91.09703*

- Exploitation

IPS

Detects and blocks exploitation of JetBrains TeamCity Authentication Bypass Vulnerability (CVE-2023-42793)

FortiGate *DB 26.685*
FortiSASE *DB 26.685*
FortiNDR *DB 26.685*
FortiADC *DB 26.685*
FortiProxy *DB 26.685*

Web App Security

Detects and blocks exploitation of JetBrains TeamCity Authentication Bypass Vulnerability (CVE-2023-42793)

FortiWeb *DB 0.00366*
FortiADC *DB 1.00048*

- Installation

Web & DNS Filter

Known related URL, IPs, Domains are rated as "Malicious "

FortiGate

- C2

Botnet C&C

Blocks communication with related malicous C2 servers and domains.

FortiGate

- Action

DETECT

Find and correlate important information to identify an outbreak, the following updates are available to raise alert and generate reports:

Outbreak Detection

FortiClient *DB 1.00017*
FortiAnalyzer *DB 2.00032*
FortiSIEM *DB 602*

RESPOND

Develop containment techniques to mitigate impacts of security events:

Automated Response

Services that can automatically respond to this outbreak.

FortiEDR

Assisted Response Services

Experts to assist you with analysis, containment and response activities.

Incident Response
FortiRecon: ACI

RECOVER

Improve security posture and processes by implementing security awareness and training, in preparation for (and recovery from) security incidents:

NOC/SOC Training

Train your network and security professionals and optimize your incident response to stay on top of the cyberattacks.

NSE Training
Response Readiness

End-User Training

Raise security awareness to your employees that are continuously being targetted by phishing, drive-by download and other forms of cyberattacks.

Security Awareness & Training

IDENTIFY

Identify processes and assets that need protection:

Attack Surface Hardening

Check Security Fabric devices to build actionable configuration recommendations and key indicators.

Security Rating

Business Reputation

Know attackers next move to protect against your business branding.

FortiRecon: EASM

Additional Resources

FortiGuard Research	https://www.fortinet.com/blog/threat-research/teamcity-intrusion-saga-apt29-suspected-exploiting-cve-2023-42793
Jetbrains Advisory	https://blog.jetbrains.com/teamcity/2023/09/critical-security-issue-affecting-teamcity-on-premises-update-to-2023-05-4-now/
CISA Advisory	https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-347a
Jetbrains Blog	https://blog.jetbrains.com/teamcity/2023/09/cve-2023-42793-vulnerability-post-mortem/

Learn more about FortiGuard Outbreak Alerts