Select ~ START TRIAL

RAPIDI

CVE-2022-**36804: Easily Exploitable Vulnerability in Atlassian Bitbucket** Server and **Data Center**

Sep 20, 2022 | 2 min read | **Ron Bowes**







Last updated at Mon, 26 Sep 2022 14:29:02 GMT

On August 24, 2022, Atlassian published an advisory for Bitbucket Server and Data



Q

Topics

Metasploit (653)

Vulnerability

Management (359)

Research (236)

Detection and Response

(205)

Vulnerability Disclosure

(148)

Emergent Threat

Response (141)

Cloud Security (136)

Security Operations (20)

Popular Tags

≡ RAPID₁ Q

Select V START TRIAL

vulnerability in multiple API endpoints, which allows an attacker with access to a public repository or with read **permissions** to a private Bitbucket repository to execute arbitrary code by sending a malicious HTTP request. CVE-2022-36804 carries a CVSSv3 score of 9.8 and is easily exploitable. Rapid7's vulnerability research team has a full technical analysis in AttackerKB \(\omega \), including how to use CVE-2022-36804 to create a simple reverse shell.

According to Shodan , there are about 1,400 internet-facing servers, but it's not immediately obvious how many have a public repository. There are no public reports of exploitation in the

Metasploit

Metasploit Weekly Wrapup

Vulnerability Management

Research

Logentries

Detection and Response

Related Posts

Fortinet

FortiManager CVE-

2024-47575

Exploited in Zero-

Day Attacks

MORE

READ

Multiple

Vulnerabilities in

Common Unix

Printing System

(CUPS)

MORE

READ

High-Risk

Vulnerabilities in

E RAPIDD ○

Select > START TRIAL

vulnerability from researchers and exploit brokers, and there are now multiple public exploits available. Because the vulnerability is trivially exploitable and the patch is relatively simple to reverseengineer, it's likely that targeted exploitation has already occurred in the wild. We expect to see larger-scale exploitation of CVE-2022-36804 soon.

Note: Several threat intelligence sources reported $\ \$ seeing exploitation attempts in the wild as of September 23, 2022.

Affected products:

Bitbucket Server and Data
Center 7.6 prior to 7.6.17
Bitbucket Server and Data
Center 7.17 prior to 7.17.10

7 V L 2024 40700

Critical Improper

Access Control

Vulnerability

Affecting SonicWall READ

Devices MORE

Q

Select >

START TRIAL

Center 8.0 prior to 8.0.3

Bitbucket Server and Data

Center 8.1 prior to 8.1.3

Bitbucket Server and Data

Center 8.2 prior to 8.2.2

Bitbucket Server and Data

Center 8.3 prior to 8.3.1

Mitigation guidance

Organizations that use
Bitbucket Server and Data
Center in their environments
should patch as quickly as
possible using Atlassian's guide

, without waiting for a regular
patch cycle to occur. Blocking
network access to Bitbucket
may also function as a
temporary stop-gap solution,
but this should not be a
substitute for patching.

≡ RAPID™

Select V START TRIAL

InsightVM and Nexpose
customers can assess their
exposure to CVE-2022-36804
with an unauthenticated
vulnerability check in the
September 20, 2022 content
release (ContentOnlycontent-1.1.2653202209202050).

A detection rule, Suspicious
Process - Atlassian
BitBucket Spawns
Suspicious Commands, was
deployed to InsightIDR around

Suspicious Commands, was deployed to InsightIDR around 10am ET on September 22, 2022.

Updates

September 22, 2022 10:00AM

ET

Updated Rapid7 customers



September 26, 2022 10:30 AM

EDT

Updated to reflect reports of exploitation in the wild.

NEVER MISS A BLOG

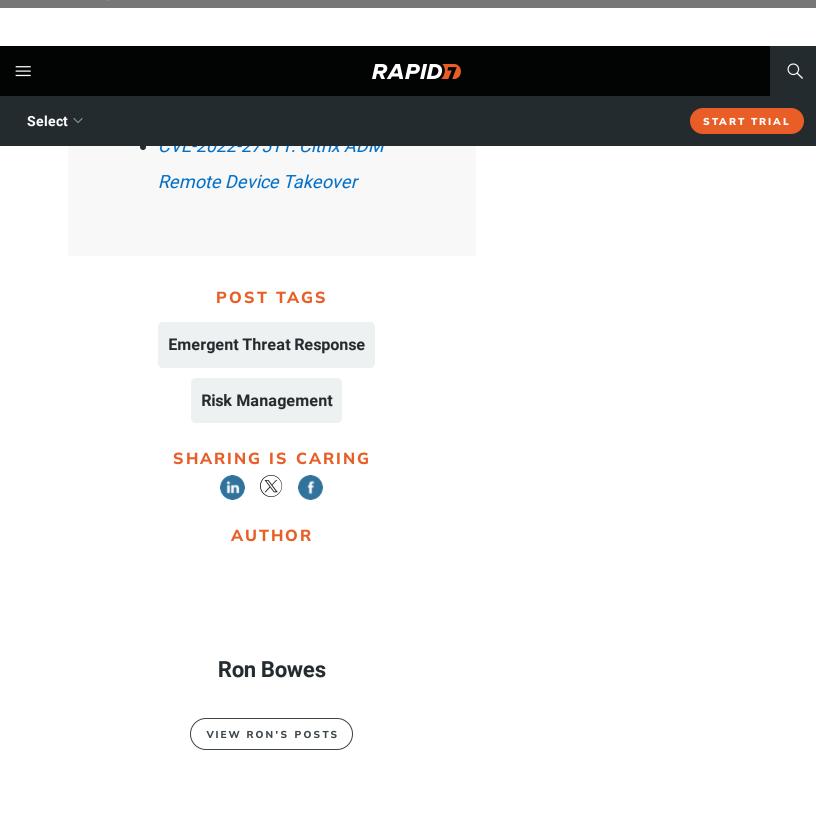
Get the latest stories, expertise, and news about security today.

SUBSCRIBE

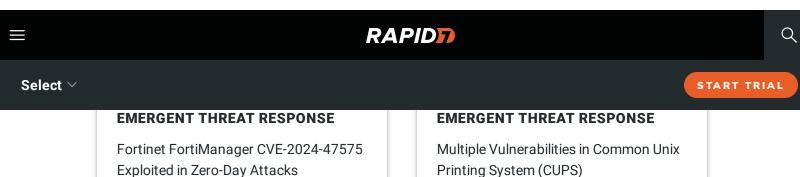
Additional reading:

- Active Exploitation of Multiple
 Vulnerabilities in Zimbra
 Collaboration Suite
- Active Exploitation of
 Atlassian's Questions for
 Confluence App CVE-2022 26138

CVE-2022-36804: Vulnerability in Atlassian Bitbucket Server and Data Center | Rapid7 Blog - 01/11/2024 12:51 https://www.rapid7.com/blog/post/2022/09/20/cve-2022-36804-easily-exploitable-vulnerability-in-atlassian-bitbucket-server-and-data-center/



Related Posts



READ FULL POST

Printing System (CUPS)

READ FULL POST

EMERGENT THREAT RESPONSE

High-Risk Vulnerabilities in Common **Enterprise Technologies**

READ FULL POST

EMERGENT THREAT RESPONSE

CVE-2024-40766: Critical Improper Access Control Vulnerability Affecting SonicWall Devices

READ FULL POST

VIEW ALL POSTS

Q Search all the things **BACK TO TOP**

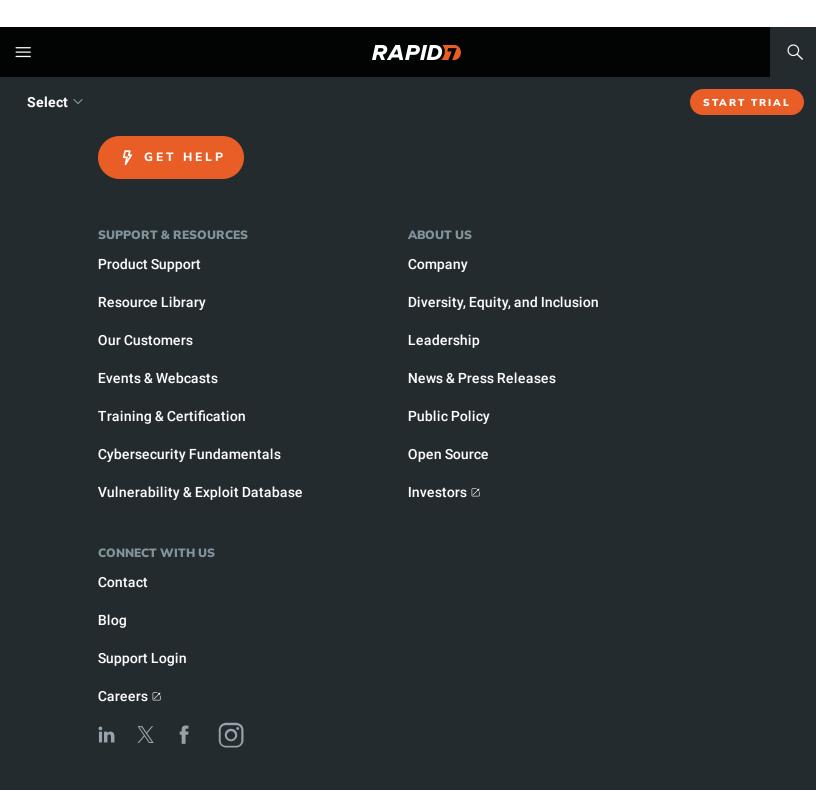
SOLUTIONS

CUSTOMER SUPPORT

+1-866-390-8113 (Toll Free)

The Command Platform

https://www.rapid7.com/blog/post/2022/09/20/cve-2022-36804-easily-exploitable-vulnerability-in-atlassian-bitbucket-server-and-data-center/



CVE-2022-36804: Vulnerability in Atlassian Bitbucket Server and Data Center | Rapid7 Blog - 01/11/2024 12:51 https://www.rapid7.com/blog/post/2022/09/20/cve-2022-36804-easily-exploitable-vulnerability-in-atlassian-bitbucket-server-and-data-center/

