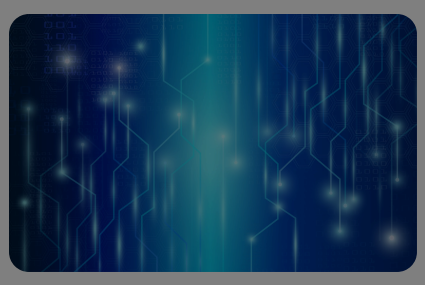

CVE-2022-36804: Easily Exploitable Vulnerability in Atlassian Bitbucket Server and Data Center

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 Center alerting users to CVE-2022-36804. The advisory reveals a command injection 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, 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 wild as of September 20, 2022 (edit: see note below), but there has been strong interest in the 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 reverse- engineer, it's likely that targeted exploitation has already occurred in the wild. We expect to see larger-scale exploitation of

Topics

Metasploit (654)

Vulnerability Management (359)

Research (236)

Detection and Response (205)

Vulnerability Disclosure (148)

Emergent Threat Response (141)

Cloud Security (136)

Security Operations (20)

Popular Tags

Search Tags

Metasploit

Metasploit Weekly Wrapup

Vulnerability Management

Research

Logentries

Detection and Response

Bitbucket Server and Data Center 7.17 prior to 7.17.10

Bitbucket Server and Data Center 7.21 prior to 7.21.4

Bitbucket Server and Data 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.

Rapid7 customers

InsightVM and Nexpose customers can assess their exposure to CVE-2022-36804 with an unauthenticated vulnerability check in the September 20, 2022 content release (`ContentOnly-content-1.1.2653-202209202050`).

A detection rule, `Suspicious Process - Atlassian BitBucket Spawns Suspicious Commands`, was deployed to InsightIDR around 10am ET on September 22, 2022.

Updates

September 22, 2022 10:00AM ET

Updated Rapid7 customers section to include information on a new IDR detection rule.

September 26, 2022 10:30 AM EDT

Updated to reflect reports of exploitation in the wild.

2024-47575 Exploited in Zero-Day Attacks READ MORE

Multiple Vulnerabilities in Common Unix Printing System (CUPS) READ MORE

High-Risk Vulnerabilities in Common Enterprise Technologies READ MORE

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

Additional reading:

- *Active Exploitation of Multiple Vulnerabilities in Zimbra Collaboration Suite*
- *Active Exploitation of Atlassian's Questions for Confluence App CVE-2022-26138*
- *Exploitation of Mitel MiVoice Connect SA CVE-2022-29499*
- *CVE-2022-27511: Citrix ADM Remote Device Takeover*

POST TAGS

Emergent Threat Response

Risk Management

SHARING IS CARING

AUTHOR

Ron Bowes

VIEW RON'S POSTS

Related Posts

EMERGENT THREA...

Fortinet FortiManager CVE-2024-47575 Exploited in Zero-Day

READ FULL POST

EMERGENT THREA...

Multiple Vulnerabilities in Common Unix Printing System

READ FULL POST

EMERGENT THREA...

High-Risk Vulnerabilities in Common Enterprise

READ FULL POST

EMERGENT THREA...

CVE-2024-40766: Critical Improper Access Control

READ FULL POST

VIEW ALL POSTS

CUSTOMER SUPPORT

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

SALES SUPPORT

+1-866-772-7437 (Toll Free)

Need to report an Escalation or a Breach?

GET HELP

The Command Platform

Exposure Command

Managed Threat Complete

RESOURCES

Product Support

Resource Library

Our Customers

Events & Webcasts

Training & Certification

Cybersecurity Fundamentals

Vulnerability & Exploit Database

Company

Diversity, Equity, and Inclusion

Leadership

News & Press Releases

Public Policy

Open Source

Investors

Contact

Blog

Support Login

Careers