



Active Exploitation of Confluence Server & Confluence Data Center: CVE-2021-26084

Sep 02, 2021 | 2 min read | [Caitlin Condon](#)





Last updated at Tue, 09 Nov 2021 20:15:30 GMT

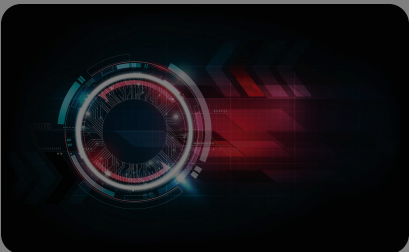
This attack is ongoing. See the [Updates](#) section at the end of this post for new information as it comes to light.

On August 25, 2021, Atlassian [published details](#)  on [CVE-2021-26084](#) , a critical remote code execution vulnerability in Confluence Server and Confluence Data Center. The vulnerability arises from an OGNL injection flaw and allows unauthenticated attackers to execute arbitrary code on Confluence Server or Data Center instances. The affected versions are before version 6.13.23, from version 6.14.0 before 7.4.11, from version 7.5.0 before 7.11.6, and from version 7.12.0 before 7.12.5.

Proof-of-concept exploit code has been publicly available since August 31, 2021, and both Rapid7 and community researchers have observed active exploitation as of September 2. **Organizations that have not patched this Confluence Server and Confluence Data Center vulnerability should do so on an emergency basis.**

For a complete list of fixed versions, see [Atlassian’s advisory here](#) .

For full vulnerability analysis, including triggers and check information, see [Rapid7’s analysis in AttackerKB](#) .



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

Accept Cookies

Decline Cookies



Rapid7 uses cookies and similar technologies as strictly necessary to make our site work. We and our partners would also like to set additional cookies to analyze your use of our site, to personalize and enhance your visit to our site and to show you more relevant content and advertising. These will be set only if you accept.

You can always review and change your cookie preferences through our cookie settings page. For more information, please read our **Privacy Statement**

Platform

Products

Services

Resources

Company

Partners

EN

Sign In

Blog

Vulnerability Management

MDR

Detection & Response

Cloud Security

App Security

Metasploit

All Topics

START TRIAL

Confluence targets. InsightIDR customers should ensure that the Insight Agent is installed on all Confluence servers to maximize post-compromise detection visibility.

InsightVM and Nexpose customers can assess their exposure to [CVE-2021-26084](#) with remote vulnerability checks as of the August 26, 2021 content release.

Updates

September 2, 2021:

The Rapid7 Threat Detection & Response team added or updated the following detections to InsightIDR to help you identify successful exploitation of this vulnerability:

Suspicious Process - Curl Downloading Shell Script

detects when the Curl utility is being used to download a shell script. The Curl utility is often used by malicious actors to download additional payloads on compromised Linux systems.

Suspicious Process - Confluence Java App Launching Processes

identifies processes being launched by the Atlassian Confluence server app. Malicious actors have been observed exploiting CVE-2021-26084, a vulnerability for Confluence disclosed in August 2021 which can allow execution of arbitrary processes.

Suspicious Process - Common Compromised Linux Webserver Commands

identifies commands that Rapid7 has observed being run on compromised Linux webservers.

September 3, 2021:

Attacks are continuing to increase, therefore Rapid7 has updated the patching priority to "patch on an emergency basis."

The US Cyber Command has tweeted guidance asking

CVE-2024-40766: Exploited in Zero-Day Attacks

Multiple Vulnerabilities in Common Unix Printing System (CUPS)

High-Risk Vulnerabilities in Common Enterprise Technologies

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

Rapid7 uses cookies and similar technologies as strictly necessary to make our site work. We and our partners would also like to set additional cookies to analyze your use of our site, to personalize and enhance your visit to our site and to show you more relevant content and advertising. These will be set only if you accept.

You can always review and change your cookie preferences through our cookie settings page. For more information, please read our **Privacy Statement**

Page 2 of 4

take long.

September 7, 2021:

Atlassian has updated their [advisory on CVE-2021-26084](#)

[❏](#) to note that the vulnerability is exploitable by unauthenticated attackers *regardless of configuration*.

Widespread exploitation is ongoing.

October 4, 2021

[Sophos is sharing details](#) [❏](#) about a ransomware attack utilizing this vulnerability to provide the attacker's initial access.

NEVER MISS A BLOG

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

SUBSCRIBE

POST TAGS

Emergent Threat Response

Risk Management

AUTHOR

Caitlin Condon

Director, Vulnerability Intelligence

VIEW CAITLIN'S POSTS

SHARING IS CARING



Related Posts

EMERGENT THREA...

EMERGENT THREA...

EMERGENT THREA...

EMERGENT THREA...

Rapid7 uses cookies and similar technologies as strictly necessary to make our site work. We and our partners would also like to set additional cookies to analyze your use of our site, to personalize and enhance your visit to our site and to show you more relevant content and advertising. These will be set only if you accept.

You can always review and change your cookie preferences through our cookie settings page. For more information, please read our **Privacy Statement**

