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*

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

Contact Us

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

Metasploit

Metasploit Weekly Wrapup

Vulnerability Management

Research

Logentries

Detection and Response

Related Posts

Fortinet FortiManager CVE-2024-47575 Exploited in Zero-Day Attacks READ MORE

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

High-Risk Vulnerabilities in

Contact Us

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.

Rapid7 customers

Rapid7's Managed Detection and Response (MDR) team has observed active exploitation against vulnerable Confluence targets. InsightIDR customers should ensure that the Insight Agent is installed on all

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

READ MORE

Contact Us

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 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.

Contact Us

updated the patching priority to "patch on an emergency basis."

The US Cyber Command has tweeted guidance asking for organizations to "patch immediately" as "this cannot wait until after the weekend."

CISA has also released a ransomware awareness guide for holidays and weekends.

Current attacks have been focused on deploying coin miners, but the pivot to deploying ransomware may not take long.

September 7, 2021: Atlassian has updated their advisory on CVE-2021-26084 to note that the vulnerability is exploitable by unauthenticated

October 4, 2021

Sophos is sharing details about a ransomware attack utilizing this vulnerability to provide the attacker's initial access.

POST TAGS

Emergent Threat Response

Risk Management

SHARING IS CARING

Contact Us

Caitlin Condon

Director, Vulnerability Intelligence

VIEW CAITLIN'S POSTS

Related Posts

EMERGENT THREAT RESPONSE

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

READ FULL POST

EMERGENT THREAT RESPONSE

Multiple Vulnerabilities in Common Unix Printing System (CUPS)

READ FULL POST

Contact Us

RAPID7

Select

START TRIAL

Enterprise Technologies

READ FULL POST

Access Control Vulnerability Affecting SonicWall Devices

READ FULL POST

VIEW ALL POSTS

Search all the things

BACK TO TOP

SOLUTIONS

The Command Platform

Exposure Command

Managed Threat Complete

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

SUPPORT & RESOURCES

Product Support

Resource Library

Our Customers

Events & Webcasts

ABOUT US

Company

Diversity, Equity, and Inclusion

Leadership

News & Press Releases

Contact Us

Select

START TRIAL

CONNECT WITH US

Contact

Blog

Support Login

Careers

Legal Terms

Privacy Policy

Export Notice

Trust

Do Not Sell or Share My Personal Information

Cookie Preferences

Contact Us