



≡ NVD MENU

[Information Technology Laboratory](#)

## NATIONAL VULNERABILITY DATABASE



VULNERABILITIES

# 🔍 CVE-2021-26084 Detail

## Description

In affected versions of Confluence Server and Data Center, an OGNL injection vulnerability exists that would allow an unauthenticated attacker to execute arbitrary code on a Confluence Server or Data Center instance. 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.

## Metrics

CVSS Version 4.0	CVSS Version 3.x	CVSS Version 2.0
------------------	------------------	------------------

NVD enrichment efforts reference publicly available information to associate vector strings. CVSS information contributed by other sources is also displayed.

**CVSS 3.x Severity and Vector Strings:**



**NIST:** NVD

**Base Score:** 9.8 CRITICAL

**Vector:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

## QUICK INFO

**CVE Dictionary Entry:**

[CVE-2021-26084](#)

**NVD Published Date:**

08/30/2021

**NVD Last Modified:**

08/08/2023

**Source:**

Atlassian

## References to Advisories, Solutions, and Tools

By selecting these links, you will be leaving NIST webspace. We have provided these links to other web sites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other web sites that are more appropriate for your purpose. NIST does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, NIST does not endorse any commercial products that may be mentioned on these sites. Please address comments about this page to [nvd@nist.gov](mailto:nvd@nist.gov).

Hyperlink	Resource
<a href="http://packetstormsecurity.com/files/167449/Atlassian-Confluence-Namespaces-OGNL-Injection.html">http://packetstormsecurity.com/files/167449/Atlassian-Confluence-Namespaces-OGNL-Injection.html</a>	Exploit
	Third Party Advisory
	VDB Entry
<a href="https://jira.atlassian.com/browse/CONFSERVER-67940">https://jira.atlassian.com/browse/CONFSERVER-67940</a>	Issue Tracking
	Patch
	Vendor Advisory


## This CVE is in CISA's Known Exploited Vulnerabilities Catalog

Reference [CISA's BOD 22-01](#) and [Known Exploited Vulnerabilities Catalog](#) for further guidance and requirements.

Vulnerability Name	Date Added	Due Date	Required Action
--------------------	------------	----------	-----------------

Atlassian Confluence Server and Data Center Object-Graph Navigation Language (OGNL) Injection Vulnerability	11/03/2021	11/17/2021	Apply updates per vendor instructions.
---	------------	------------	---

## Weakness Enumeration


CWE-ID	CWE Name	Source
CWE-917	Improper Neutralization of Special Elements used in an Expression Language Statement ('Expression La	 NIST

## Known Affected Software

### Configurations [Switch to CPE 2.2](#)

Configuration 1 ([hide](#))

 <b>cpe:2.3:a:atlassian:confluence_data_center:*:*:*:*:*:*</b> <a href="#">Show Matching CPE(s)</a> ▼	Up to (excluding) <b>6.13.23</b>	
 <b>cpe:2.3:a:atlassian:confluence_data_center:*:*:*:*:*:*</b> <a href="#">Show Matching CPE(s)</a> ▼	From (including) <b>6.14.0</b>	Up to (excluding) <b>7.4.11</b>
 <b>cpe:2.3:a:atlassian:confluence_data_center:*:*:*:*:*:*</b> <a href="#">Show Matching CPE(s)</a> ▼	From (including) <b>7.5.0</b>	Up to (excluding) <b>7.11.6</b>
 <b>cpe:2.3:a:atlassian:confluence_data_center:*:*:*:*:*:*</b> <a href="#">Show Matching CPE(s)</a> ▼	From (including) <b>7.12.0</b>	Up to (excluding) <b>7.12.5</b>
 <b>cpe:2.3:a:atlassian:confluence_server:*:*:*:*:*:*</b> <a href="#">Show Matching CPE(s)</a> ▼	Up to (excluding) <b>6.13.23</b>	
 <b>cpe:2.3:a:atlassian:confluence_server:*:*:*:*:*:*</b> <a href="#">Show Matching CPE(s)</a> ▼	From (including) <b>6.14.0</b>	Up to (excluding) <b>7.4.11</b>
 <b>cpe:2.3:a:atlassian:confluence_server:*:*:*:*:*:*</b> <a href="#">Show Matching CPE(s)</a> ▼	From (including) <b>7.5.0</b>	Up to (excluding) <b>7.11.6</b>
 <b>cpe:2.3:a:atlassian:confluence_server:*:*:*:*:*:*</b> <a href="#">Show Matching CPE(s)</a> ▼	From (including) <b>7.12.0</b>	Up to (excluding) <b>7.12.5</b>

 Denotes Vulnerable Software

[Are we missing a CPE here? Please let us know](#)



**HEADQUARTERS**  
100 Bureau Drive  
Gaithersburg, MD 20899  
(301) 975-2000

[Webmaster](#) | [Contact Us](#) | [Our Other Offices](#)



**Incident Response Assistance and Non-NVD Related  
Technical Cyber Security Questions:**  
US-CERT Security Operations Center  
Email: [soc@us-cert.gov](mailto:soc@us-cert.gov)  
Phone: 1-888-282-0870