An official website of the United States government Here's how you know

= NVD MENU

<u>Information Technology Laboratory</u>

NATIONAL VULNERABILITY DATABASE

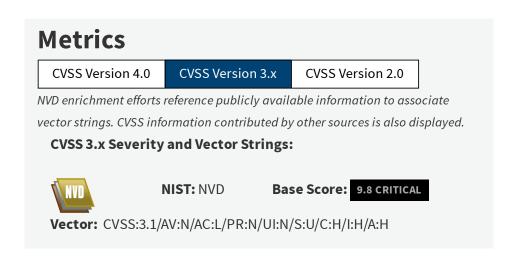


VULNERABILITIES

¥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.



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.



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

QUICK INFO

CVE Dictionary Entry:

CVE-2021-26084

NVD Published Date:

08/30/2021

NVD Last Modified:

08/08/2023

Source:

Atlassian

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

Weakness Enumeration

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

Known Affected Software Configurations Switch to CPE 2.2

Configuration 1 (hide)

Configuration 1 (<u>hide</u>)		
₩	Up to	
cpe:2.3:a:atlassian:confluence_data_center:*:*:*:*:*:*:	(excluding)	
<u>Show Matching CPE(s)</u> ▼	6.13.23	
₩.	From	Up to
cpe:2.3:a:atlassian:confluence_data_center:*:*:*:*:*:*:	(including)	(excluding)
Show Matching CPE(s)▼	6.14.0	7.4.11
₩	From	Up to
cpe:2.3:a:atlassian:confluence_data_center:*:*:*:*:*:*:	(including)	(excluding)
Show Matching CPE(s).▼	7.5.0	7.11.6
₩	From	Up to
cpe:2.3:a:atlassian:confluence_data_center:*:*:*:*:*:*:	(including)	(excluding)
Show Matching CPE(s)▼	7.12.0	7.12.5
# cpe:2.3:a:atlassian:confluence_server:*:*:*:*:*:*	Up to	
Show Matching CPE(s)▼	(excluding)	
	6.13.23	
# cpe:2.3:a:atlassian:confluence_server:*:*:*:*:*:*	From	Up to
Show Matching CPE(s)▼	(including)	(excluding)
	6.14.0	7.4.11
# cpe:2.3:a:atlassian:confluence_server:*:*:*:*:*:*	From	Up to
Show Matching CPE(s)▼	(including)	(excluding)
	7.5.0	7.11.6
# cpe:2.3:a:atlassian:confluence_server:*:*:*:*:*:*	From	Up to
Show Matching CPE(s)▼	(including)	(excluding)
	7.12.0	7.12.5

₩ Denotes Vulnerable Software

Are we missing a CPF 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
Phone: 1-888-282-0870

Site Privacy | Accessibility | Privacy Program | Copyrights | Vulnerability Disclosure | No Fear Act Policy | FOIA | Environmental Policy | Scientific Integrity | Information Quality Standards | Commerce.gov | Science.gov | USA.gov