

VULNERABILITIES

CVE-2019-3396 Detail

Current Description

The Widget Connector macro in Atlassian Confluence Server before version 6.6.12 (the fixed version for 6.6.x), from version 6.7.0 before 6.12.3 (the fixed version for 6.12.x), from version 6.13.0 before 6.13.3 (the fixed version for 6.13.x), and from version 6.14.0 before 6.14.2 (the fixed version for 6.14.x), allows remote attackers to achieve path traversal and remote code execution on a Confluence Server or Data Center instance via server-side template injection.

Source: MITRE

[View Analysis Description](#)

Severity

CVSS Version 3.x

CVSS Version 2.0

CVSS 3.x Severity and Metrics:



NIST: NVD

Base Score: 9.8 CRITICAL

Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

QUICK INFO

CVE Dictionary Entry:

[CVE-2019-3396](#)

NVD Published Date:

03/25/2019

NVD Last Modified:

04/22/2019

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.

Hyperlink	Resource
http://packetstormsecurity.com/files/152568/Atlassian-Confluence-Widget-Connector-Macro-Velocity-Template-Injection.html	Exploit Third Party Advisory VDB Entry
http://www.rapid7.com/db/modules/exploit/multi/http/confluence_widget_connector	Exploit Third Party Advisory VDB Entry
https://jira.atlassian.com/browse/CONFSERVER-57974	Issue Tracking Patch Vendor Advisory
https://www.exploit-db.com/exploits/46731/	Exploit Third Party Advisory VDB Entry

Weakness Enumeration

CWE-ID	CWE Name	Source
CWE-22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	NIST

Known Affected Software Configurations [Switch to CPE 2.2](#)Configuration 1 [\(hide\)](#)

✖ cpe:2.3:a:atlassian:confluence:*:*:*:*:*:* Show Matching CPE(s) ▼	Up to (excluding)	
	6.6.12	
✖ cpe:2.3:a:atlassian:confluence:*:*:*:*:*:* Show Matching CPE(s) ▼	From (including)	Up to (excluding)
	6.7.0	6.12.3
✖ cpe:2.3:a:atlassian:confluence:*:*:*:*:*:* Show Matching CPE(s) ▼	From (including)	Up to (excluding)
	6.13.0	6.13.3
✖ cpe:2.3:a:atlassian:confluence:*:*:*:*:*:* Show Matching CPE(s) ▼	From (including)	Up to (excluding)
	6.14.0	6.14.2

Change History

5 change records found - [show changes](#)



National Institute of
Standards and Technology
U.S. Department of Commerce



HEADQUARTERS

100 Bureau Drive
Gaithersburg, MD 20899

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

GENERAL	VULNERABILITY METRICS	CONTACT NVD	Information Technology Laboratory (ITL) National Vulnerability Database (NVD)
NVD Dashboard	CVSS V3 Calculator	OTHER SITES	Announcement and Discussion Lists
News	CVSS V2 Calculator	Checklist (NCP) Repository	General Questions & Webmaster Contact
Email List	PRODUCTS	800-53 Controls	Email: nvd@nist.gov
FAQ	CPE Dictionary	SCAP Validated Tools	
Visualizations	CPE Search	SCAP	
VULNERABILITIES	CPE Statistics	USGCB	Incident Response Assistance and Non-NVD Related
Search & Statistics	SWID	SEARCH	Technical Cyber Security Questions:
Full Listing	CONFIGURATIONS (CCE)	Vulnerability Search	US-CERT Security Operations Center
Categories		CPE Search	Email: soc@us-cert.gov
Data Feeds			Phone: 1-888-282-0870
Vendor Comments			Sponsored by DHS/NCCIC/US-CERT

