

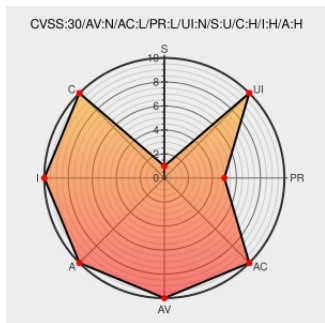


CVE-2019-3394

Published on: 08/29/2019 12:00:00 AM UTC

Last Modified on: 12/13/2021 04:05:00 PM UTC

CVE-2019-3394

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Confluence](#) from [Atlassian](#) contain the following vulnerability:

There was a local file disclosure vulnerability in Confluence Server and Confluence Data Center via page exporting. An attacker with permission to editing a page is able to exploit this issue to read arbitrary file on the server under <install-directory>/confluence/WEB-INF directory, which may contain configuration files used for integrating

with other services, which could potentially leak credentials or other sensitive information such as LDAP credentials. The LDAP credential will be potentially leaked only if the Confluence server is configured to use LDAP as user repository. All versions of Confluence Server from 6.1.0 before 6.6.16 (the fixed version for 6.6.x), from 6.7.0 before 6.13.7 (the fixed version for 6.13.x), and from 6.14.0 before 6.15.8 (the fixed version for 6.15.x) are affected by this vulnerability.

CVE-2019-3394 has been assigned by [security@atlassian.com](#) to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **8.8 - HIGH**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	LOW	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: **4 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	NONE	NONE

CVE References

Description	Tags	Link
Confluence Security Advisory - 2019-08-28 Confluence Data Center and Server 7.11 Atlassian Documentation	Patch Vendor Advisory confluence.atlassian.com text/html	 MISC confluence.atlassian.com/x/uAsvOg
[CONFSERVER-58734] Local File Disclosure via Word Export in Confluence Server - CVE-2019-3394 - Create and track feature requests for Atlassian products.	Vendor Advisory jira.atlassian.com text/html	 MISC jira.atlassian.com/browse/CONFSERVER-58734

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites 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 websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Exploit/POC from Github

Confluence (<install-directory>/confluence/WEB-INF/) 文件读取漏洞

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Atlassian	Confluence	All	All	All	All
Application	Atlassian	Confluence	All	All	All	All
Application	Atlassian	Confluence Server	All	All	All	All
cpe:2.3:a:atlassian:confluence:*.?:*.?:*.?:*.?:*.?:*.?:*.*						
cpe:2.3:a:atlassian:confluence:*.?:*.?:*.?:*.?:*.?:*.?:*.*						
cpe:2.3:a:atlassian:confluence_server:*.?:*.?:*.?:*.?:*.?:*.?:*.*						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @ipssignatures	It's new to me that Hillstone has a protection/signature/rule for the vulnerability CVE-2019-3394.... twitter.com/i/web/status/1...	2021-08-09 05:02:01
 @ipssignatures	I know 3 other IPSs that have protections/signatures/rules for the vulnerability CVE-2019-3394. ipssignatures.appspot.com/?cve=CVE-2019-... #Sgfvhulxit7fxc	2021-08-09 05:02:01

© [CVE.report](#) 2023   |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)