

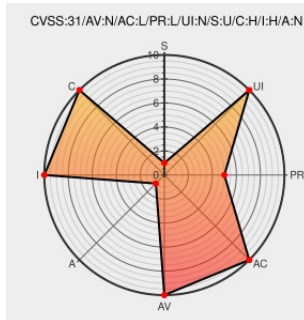


CVE-2022-35291

Published on: Not Yet Published

Last Modified on: 08/02/2022 08:09:00 PM UTC

CVE-2022-35291

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

Certain versions of [Successfactors Mobile](#) from [Sap](#) contain the following vulnerability:

Due to misconfigured application endpoints, SAP SuccessFactors attachment APIs allow attackers with user privileges to perform activities with admin privileges over the network. These APIs were consumed in the SF Mobile application for Time Off, Time Sheet, EC Workflow, and Benefits. On successful exploitation, the attacker can read/write attachments. Thus, compromising the confidentiality and integrity of the application

CVE-2022-35291 has been assigned by [SAP](#) cna@sap.com to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: [SAP](#) **SAP SuccessFactors - SAP SuccessFactors Mobile Application for Android & iOS devices** version **< V8.0.5**

CVSS3 Score: **8.1 - HIGH**

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

CVE References

Description	Tags	Link
No Description Provided	launchpad.support.sap.com text/html	SAP MISC launchpad.support.sap.com/#!/notes/3226411
Access Denied	www.sap.com text/html Inactive Link Not Archived	SAP MISC www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html

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

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Sap	Successfactors Mobile	8.0.5	All	All	All
Application	Sap	Successfactors Mobile	8.0.5	All	All	All
cpe:2.3:a:sap:successfactors_mobile:8.0.5:*:*:*:android:*:*:						
cpe:2.3:a:sap:successfactors_mobile:8.0.5:*:*:*:iphone_os:*:*:						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @CVEreport	CVE-2022-35291 : Due to misconfigured application endpoints, #SAP SuccessFactors attachment APIs allow attackers wi... twitter.com/i/web/status/1...	2022-07-27 14:08:50

[← Previous ID](#)

[Next ID→](#)