



CVE-2021-40498

Published on: 10/12/2021 12:00:00 AM UTC

Last Modified on: 10/18/2021 08:53:00 PM UTC

CVE-2021-40498

Source: Mitre

Source: Nist

Print: PDF



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

A vulnerability has been identified in SAP SuccessFactors Mobile Application for Android - versions older than 2108, which allows an attacker to prevent legitimate users from accessing a service, either by crashing or flooding the service, which can lead to denial of service.

The vulnerability is related to Android implementation methods that are widely used across Android mobile applications, and such methods are embedded into the SAP SuccessFactors mobile application. These Android methods begin executing once the user accesses their profile on the mobile application. While executing, it can also pick up the activities from other Android applications that are running in the background of the users device and are using the same types of methods in the application. Such vulnerability can also lead to phishing attacks that can be used for staging other types of attacks.

CVE-2021-40498 has been assigned by [cna@sap.com](#) to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: [SAP SE](#) - [SAP SuccessFactors Mobile Application \(for Android devices\)](#) version < 2108

CVSS3 Score: **5.5 - MEDIUM**

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

CVSS2 Score: **2.1 - LOW**

| Access Vector | Access Complexity | Authentication |
|------------------------|-------------------|---------------------|
| LOCAL | LOW | NONE |
| Confidentiality Impact | Integrity Impact | Availability Impact |
| | | |

NONE

NONE

PARTIAL

CVE References

| Description | Tags | Link |
|---|--|--|
| SAP Security Patch Day – October 2021 - Product Security Response at SAP - Community Wiki | wiki.scn.sap.com text/html | <input type="checkbox"/> MISC wiki.scn.sap.com/wiki/pages/viewpage.action?pageId=587169983 |
| No Description Provided | launchpad.support.sap.com text/html | <input checked="" type="checkbox"/> MISC launchpad.support.sap.com/#/notes/3077635 |

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.

Related QID Numbers

630754 SAP SuccessFactors For Android Insufficient Information Vulnerability

Known Affected Configurations (CPE V2.3)

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

No vendor comments have been submitted for this CVE

Social Mentions

| Source | Title | Posted (UTC) |
|------------|--|---------------------|
| @CVEreport | CVE-2021-40498 : A vulnerability has been identified in #SAP SuccessFactors Mobile Application for Android - versio... twitter.com/i/web/status/1... | 2021-10-12 14:44:16 |

← Previous ID

Next ID →

© CVE.report 2022 |

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