



CVE-2021-38150

Published on: 09/14/2021 12:00:00 AM UTC

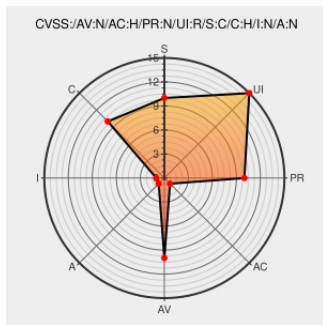
Last Modified on: 09/23/2021 07:56:00 PM UTC

CVE-2021-38150

Source: Mitre

Source: Nist

Print: PDF



Certain versions of [Business Client](#) from [Sap](#) contain the following vulnerability:

When an attacker manages to get access to the local memory, or the memory dump of a victim, for example by a social engineering attack, SAP Business Client versions - 7.0, 7.70, will allow him to read extremely sensitive data, such as credentials. This would allow the attacker to compromise the corresponding backend for which the

credentials are valid.

CVE-2021-38150 has been assigned by [cna@sap.com](#) to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: [SAP SE](#) - [SAP Business Client](#) version 7.0

Affected Vendor/Software: [SAP SE](#) - [SAP Business Client](#) version 7.70

CVSS3 Score: **6.5 - MEDIUM**

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

CVSS2 Score: **4.3 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	NONE	NONE

CVE References

Description	Tags	Link
SAP Security Patch Day – September 2021 - Product Security Response at SAP - Community Wiki	wiki.scn.sap.com text/html	SAP MISC wiki.scn.sap.com/wiki/pages/viewpage.action?pageId=585106405

No Description Provided

launchpad.support.sap.com
[text/html](#)

[SAP MISC
launchpad.support.sap.com/#/notes/3060621](https://launchpad.support.sap.com/#/notes/3060621)

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	Business Client	7.0	All	All	All
Application	Sap	Business Client	7.70	All	All	All

cpe:2.3:a:sap:business_client:7.0:*:*:*:*:*:*:

cpe:2.3:a:sap:business_client:7.70:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2021-38150 : When an attacker manages to get access to the local memory, or the memory dump of a victim, for ex... twitter.com/i/web/status/1...	2021-09-14 12:10:20

[← Previous ID](#)

[Next ID →](#)

© CVE.report 2021 [Twitter](#) [N](#) |

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