



CVE-2020-6302

Published on: 09/09/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:05 PM UTC

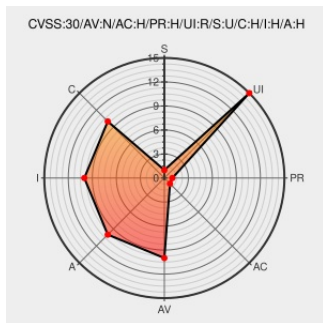
CVE-2020-6302

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



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

SAP Commerce versions 6.7, 1808, 1811, 1905, 2005 contains the jSession ID in the backoffice URL when the application is loaded initially. An attacker can get this session ID via shoulder surfing or man in the middle attack and subsequently get access to admin user accounts, leading to Session Fixation and complete compromise of the confidentiality, integrity and availability of the application.

CVE-2020-6302 has been assigned by [sap](#) cna@sap.com to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: [SAP](#) **SAP SE - SAP Commerce version 6.7**

Affected Vendor/Software: [SAP](#) **SAP SE - SAP Commerce version 1808**

Affected Vendor/Software: [SAP](#) **SAP SE - SAP Commerce version 1811**

Affected Vendor/Software: [SAP](#) **SAP SE - SAP Commerce version 1905**

Affected Vendor/Software: [SAP](#) **SAP SE - SAP Commerce version 2005**

CVSS3 Score: **8.1 - HIGH**

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

CVSS2 Score: **7.5 - HIGH**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE

Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
SAP Security Patch Day – September 2020 - Product Security Response at SAP - Community Wiki	Vendor Advisory wiki.scn.sap.com text/html	SAP MISC wiki.scn.sap.com/wiki/pages/viewpage.action?pageId=557449700
No Description Provided	Permissions Required launchpad.support.sap.com text/html	SAP MISC launchpad.support.sap.com/#/notes/2934451

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	Commerce	1808	All	All	All
Application	Sap	Commerce	1811	All	All	All
Application	Sap	Commerce	1905	All	All	All
Application	Sap	Commerce	2005	All	All	All
Application	Sap	Commerce	6.7	All	All	All
Application	Sap	Commerce	1808	All	All	All
Application	Sap	Commerce	1811	All	All	All
Application	Sap	Commerce	1905	All	All	All
Application	Sap	Commerce	2005	All	All	All
Application	Sap	Commerce	6.7	All	All	All

cpe:2.3:a:sap:commerce:1808:*****:

cpe:2.3:a:sap:commerce:1811:*****:

cpe:2.3:a:sap:commerce:1905:*****:

cpe:2.3:a:sap:commerce:2005:*****:

cpe:2.3:a:sap:commerce:6.7:*****:

cpe:2.3:a:sap:commerce:1808:*****:

cpe:2.3:a:sap:commerce:1811:*****:

cpe:2.3:a:sap:commerce:1905:*****:
cpe:2.3:a:sap:commerce:2005:*****:
cpe:2.3:a:sap:commerce:6.7:*****:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

© [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](#)