

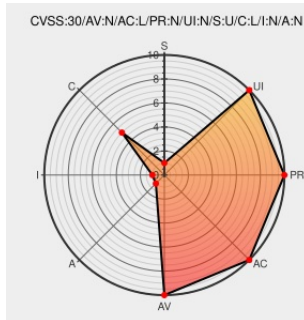


# CVE-2020-26811

Published on: 11/10/2020 12:00:00 AM UTC

Last Modified on: 06/17/2021 05:20:00 PM UTC

## CVE-2020-26811

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

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

SAP Commerce Cloud (Accelerator Payment Mock), versions - 1808, 1811, 1905, 2005, allows an unauthenticated attacker to submit a crafted request over a network to a particular SAP Commerce module URL which will be processed without further interaction, the crafted request leads to Server Side Request Forgery attack which could lead

to retrieval of limited pieces of information about the service with no impact on integrity or availability.

CVE-2020-26811 has been assigned by [SAP](#) cna@sap.com to track the vulnerability - currently rated as **MEDIUM** severity.

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

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

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

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

CVSS3 Score: **5.3 - MEDIUM**

| Attack Vector    | Attack Complexity      | Privileges Required | User Interaction    |
|------------------|------------------------|---------------------|---------------------|
| <b>NETWORK</b>   | <b>LOW</b>             | <b>NONE</b>         | <b>NONE</b>         |
| Scope            | Confidentiality Impact | Integrity Impact    | Availability Impact |
| <b>UNCHANGED</b> | <b>LOW</b>             | <b>NONE</b>         | <b>NONE</b>         |

CVSS2 Score: **5 - MEDIUM**

| Access Vector          | Access Complexity | Authentication      |
|------------------------|-------------------|---------------------|
| <b>NETWORK</b>         | <b>LOW</b>        | <b>NONE</b>         |
| <b>Confidentiality</b> | <b>Integrity</b>  | <b>Availability</b> |

| Impact  | Impact | Impact |
|---------|--------|--------|
| PARTIAL | NONE   | NONE   |

| CVE References                                                                                                                     |                                                                                                                |                                                                                                                                                                                                                                                                                                         |
|------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Description                                                                                                                        | Tags                                                                                                           | Link                                                                                                                                                                                                                                                                                                    |
| Full Disclosure: Onapsis Security Advisory 2021-0006: [CVE-2020-26811] - SAP Hybris eCommerce - SSRF in acceleratorservices module | <a href="#">seclists.org</a><br><a href="#">text/html</a>                                                      |  FULLDISC 20210614 Onapsis Security Advisory 2021-0006: [CVE-2020-26811] - SAP Hybris eCommerce - SSRF in acceleratorservices module                                                                                 |
| SAP Security Patch Day – November 2020 - Product Security Response at SAP - Community Wiki                                         | <a href="#">Vendor Advisory</a><br><a href="#">wiki.scn.sap.com</a><br><a href="#">text/html</a>               |  MISC<br><a href="https://wiki.scn.sap.com/wiki/pages/viewpage.action?pageId=562725571">wiki.scn.sap.com/wiki/pages/viewpage.action?pageId=562725571</a>                                                             |
| SAP Hybris eCommerce Server-Side Request Forgery ~ Packet Storm                                                                    | <a href="#">packetstormsecurity.com</a><br><a href="#">text/html</a>                                           |  MISC<br><a href="https://packetstormsecurity.com/files/163143/SAP-Hybris-eCommerce-Server-Side-Request-Forgery.html">packetstormsecurity.com/files/163143/SAP-Hybris-eCommerce-Server-Side-Request-Forgery.html</a> |
| No Description Provided                                                                                                            | <a href="#">Permissions Required</a><br><a href="#">launchpad.support.sap.com</a><br><a href="#">text/html</a> |  MISC<br><a href="https://launchpad.support.sap.com/#/notes/2975170">launchpad.support.sap.com/#/notes/2975170</a>                                                                                                   |

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](mailto: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 Cloud Accelerator Payment Mock | 1808    | All    | All     | All      |
| Application                              | Sap    | Commerce Cloud Accelerator Payment Mock | 1811    | All    | All     | All      |
| Application                              | Sap    | Commerce Cloud Accelerator Payment Mock | 1905    | All    | All     | All      |
| Application                              | Sap    | Commerce Cloud Accelerator Payment Mock | 2005    | All    | All     | All      |
| Application                              | Sap    | Commerce Cloud Accelerator Payment Mock | 1808    | All    | All     | All      |
| Application                              | Sap    | Commerce Cloud Accelerator Payment Mock | 1811    | All    | All     | All      |
| Application                              | Sap    | Commerce Cloud Accelerator Payment Mock | 1905    | All    | All     | All      |
| Application                              | Sap    | Commerce Cloud Accelerator Payment Mock | 2005    | All    | All     | All      |

cpe:2.3:a:sap:commerce\_cloud\_(accelerator\_payment\_mock):1808:\*\*\*\*\*:

cpe:2.3:a:sap:commerce\_cloud\_(accelerator\_payment\_mock):1811:\*\*\*\*\*:

cpe:2.3:a:sap:commerce\_cloud\_(accelerator\_payment\_mock):1905:\*\*\*\*\*:

cpe:2.3:a:sap:commerce\_cloud\_(accelerator\_payment\_mock):2005:\*\*\*\*\*:

|                                                                         |
|-------------------------------------------------------------------------|
| cpe:2.3:a:sap:commerce_cloud_(accelerator_payment_mock):1806: : : : : : |
| cpe:2.3:a:sap:commerce_cloud_(accelerator_payment_mock):1811: : : : : : |
| cpe:2.3:a:sap:commerce_cloud_(accelerator_payment_mock):1905: : : : : : |
| cpe:2.3:a:sap:commerce_cloud_(accelerator_payment_mock):2005: : : : : : |

No vendor comments have been submitted for this CVE

#### Social Mentions

| Source                                                                                            | Title                                                                                                                                                               | Posted (UTC)        |
|---------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------|
|  @SecurityNewsbot | #Onapsis #Security #Advisory 2021-0006: [CVE-2020-26811] - SAP Hybris eCommerce - SSRF in acceler... <a href="#">seclists.org/fulldisclosure...</a> #FullDisclosure | 2021-06-14 17:15:09 |
|  @GetinfosecN     | Onapsis Security Advisory 2021-0006: [CVE-2020-26811] - SAP Hybris eCommerce - SSRF in acceleratorservices modu..... <a href="#">twitter.com/i/web/status/1...</a>  | 2021-06-14 22:10:23 |

[← 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](#)