



CVE-2022-22530

Published on: 01/14/2022 12:00:00 AM UTC

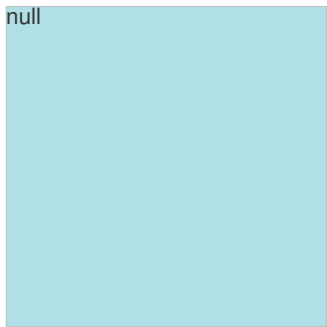
Last Modified on: 01/21/2022 09:07:00 PM UTC

CVE-2022-22530

Source: Mitre

Source: Nist

Print: PDF



Certain versions of [S/4hana](#) from [Sap](#) contain the following vulnerability:

The F0743 Create Single Payment application of SAP S/4HANA - versions 100, 101, 102, 103, 104, 105, 106, does not check uploaded or downloaded files. This allows an attacker with basic user rights to inject dangerous content or malicious code which could result in critical information being modified or completely compromise the availability of the application.

CVE-2022-22530 has been assigned by [sap](#) cna@sap.com to track the vulnerability - currently rated as **HIGH** severity.

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	NONE	HIGH	HIGH

CVSS2 Score: **7.5 - HIGH**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE
Confidentiality Impact	Integrity Impact	Availability Impact
NONE	PARTIAL	COMPLETE

CVE References

Description	Tags	Link
SAP Security Patch Day – January 2022 - 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?

No Description Provided

launchpad.support.sap.com

 MISC

[text/html](#)

launchpad.support.sap.com/#/notes/3112928

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	S/4hana	100	All	All	All
Application	Sap	S/4hana	101	All	All	All
Application	Sap	S/4hana	102	All	All	All
Application	Sap	S/4hana	103	All	All	All
Application	Sap	S/4hana	104	All	All	All
Application	Sap	S/4hana	105	All	All	All
Application	Sap	S/4hana	106	All	All	All

<code>cpe:2.3:a:sap:s/4hana:100:*:*:*:*:*:</code>
<code>cpe:2.3:a:sap:s/4hana:101:*:*:*:*:*:</code>
<code>cpe:2.3:a:sap:s/4hana:102:*:*:*:*:*:</code>
<code>cpe:2.3:a:sap:s/4hana:103:*:*:*:*:*:</code>
<code>cpe:2.3:a:sap:s/4hana:104:*:*:*:*:*:</code>
<code>cpe:2.3:a:sap:s/4hana:105:*:*:*:*:*:</code>
<code>cpe:2.3:a:sap:s/4hana:106:*:*:*:*:*:</code>

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @CVEreport	CVE-2022-22530 : The F0743 Create Single Payment application of #SAP S/4HANA - versions 100, 101, 102, 103, 104, 10... twitter.com/i/web/status/1...	2022-01-14 20:08:54
 @SecRiskRptSME	RT: CVE-2022-22530 The F0743 Create Single Payment application of SAP S/4HANA - versions 100, 101, 102, 103, 104,... twitter.com/i/web/status/1...	2022-01-15 08:33:52

[← 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