



CVE-2021-23631

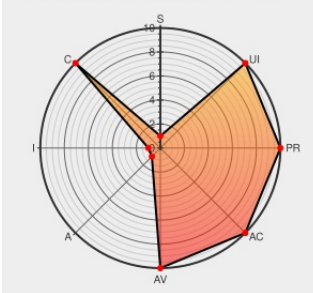
Published on: 01/21/2022 12:00:00 AM UTC

Last Modified on: 01/27/2022 07:03:00 PM UTC

CVE-2021-23631

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

CVSS:31/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N/E:P



Certain versions of [Convert-svg-core](#) from [Convert-svg-core Project](#) contain the following vulnerability:

This affects all versions of package convert-svg-core; all versions of package convert-svg-to-png; all versions of package convert-svg-to-jpeg. Using a specially crafted SVG file, an attacker could read arbitrary files from the file system and then show the file content as a converted PNG file.

CVE-2021-23631 has been assigned by report@snyk.io to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **7.5 - HIGH**

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

CVSS2 Score: **5 - MEDIUM**

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

CVE References

Description	Tags	Link
Directory Traversal in convert-svg-core CVE-2021-23631 Snyk	snyk.io text/html	MISC snyk.io/vuln/SNYK-JS-CONVERTSVGCORE-1582785
Proof of Concept for CVE-2021-23631	gist.github.com	MISC

gists.githu...
text/html

 gist.github.com/legndery/a248350bb25b8502a03c2f407cedeb14

Directory Traversal in convert-svg-to-jpeg | CVE-2021-23631 | Snyk

snyk.io
text/html

 MISC snyk.io/vuln/SNYK-JS-CONVERTSVGTOJPEG-2348245

Directory Traversal in convert-svg-to-png | CVE-2021-23631 | Snyk

snyk.io
text/html

 MISC snyk.io/vuln/SNYK-JS-CONVERTSVGTOPNG-2348244

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	Convert-svg-core Project	Convert-svg-core	All	All	All	All

cpe:2.3:a:convert-svg-core_project:convert-svg-core:*:*:*:*:node.js:*:*:

Discovery Credit

Aritra Chakraborty

Social Mentions

Source	Title	Posted (UTC)
 @CVEreport	CVE-2021-23631 : This affects all versions of package convert-svg-core; all versions of package convert-svg-to-png;... twitter.com/i/web/status/1...	2022-01-21 20:13:28
 @WesUncensored	New vulnerability on the NVD: CVE-2021-23631 ift.tt/3IHZPZ	2022-01-21 21:49:44
 @xanadulinux	CVE-2021-23631 ift.tt/3IHZPZ	2022-01-21 22:06:04
 /r/netcve	CVE-2021-23631	2022-01-21 21:54:38

← Previous ID

Next ID →

© CVE.report 2024   |

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](#)