Stored Cross Site Scripting (XSS) via malicious SVG Icon Upload

Moderate **ajinabraham** published **GHSA-mwfg-948f-2cc5** 2 days ago

Package	Affected versions	Patched versions
mobsf (pip)	<=4.3.2	4.3.3

Description

Vulnerable MobSF Versions: <= v4.3.2

CVSS V4.0 Score: 8.6
(CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:P/VC:H/VI:H/VA:L/SC:N/SI:N/SA:N)

Details:
A Stored Cross-Site Scripting (XSS) vulnerability has been identified in MobSF versions ≤ 4.3.2. The vulnerability arises from improper sanitization of user-supplied SVG files during the Android APK analysis workflow.

When an Android Studio project contains a malicious SVG file as an app icon (e.g path, /app/src/main/res/mipmap-hdpi/ic_launcher.svg), and the project is zipped and uploaded to MobSF, the tool processes and extracts the contents without validating or sanitizing the SVG.

Upcon ZIP extraction this icon file is saved by MobSF to:
user/.MobSF/downloads/.svg

This file becomes publicly accessible via the web interface at:

http://127.0.0.1:8081/download/filename.svg

If the SVG contains embedded JavaScript (e.g., an XSS payload), accessing this URL via a browser leads to the execution of the script in the context of the MobSF user session, resulting in stored XSS.

Proof Of Concept:

1. Create a malicious SVG file (ic_launcher.svg) with an embedded XSS payload.

Severity

Moderate 6.8 / 10

CVSS v4 base metrics

Exploitability Metrics

Attack Vector	Network
Attack Complexity	Low
Attack Requirements	None
Privileges Required	High
User interaction	Active

Vulnerable System Impact Metrics

Confidentiality	High
Integrity	Low
Availability	None

Subsequent System Impact Metrics

Confidentiality	None
Integrity	None
Availability	None

Learn more about base metrics

CVSS:4.0/AV:N/AC:L/AT:N/PR:H/UI:A/VC:H/VI:L/VA:N/SC:N/SI:N/SA:N

CVE ID

CVE-2025-46335

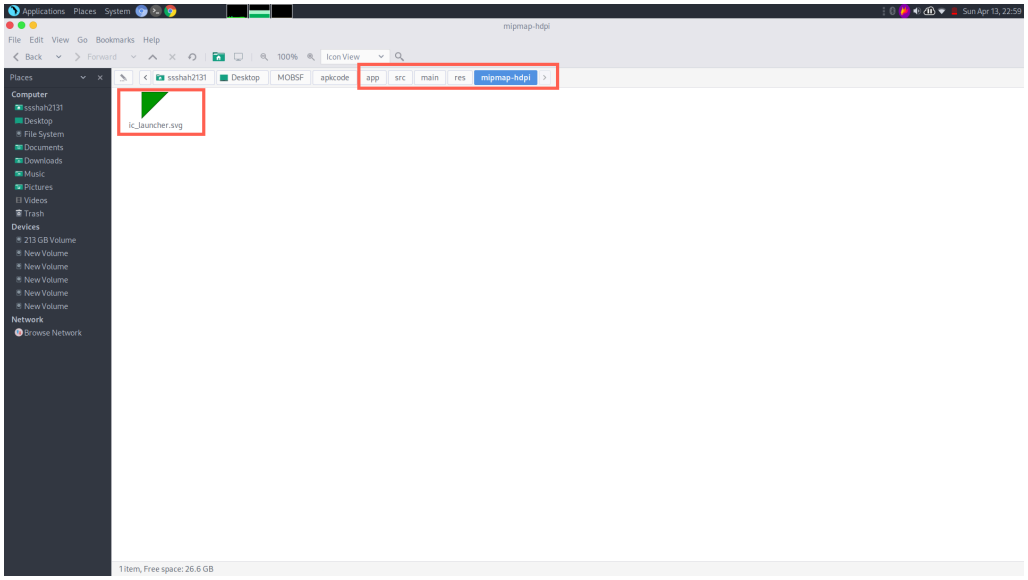
Weaknesses

ic_launcher.svg

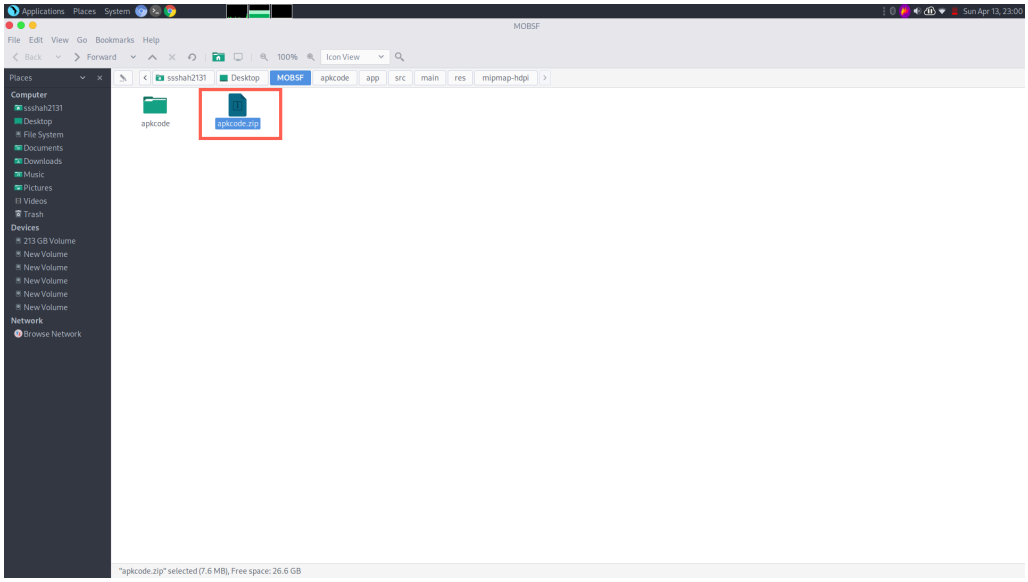
```svg
<?xml version="1.0" standalone="no"?>
<!DOCTYPE svg PUBLIC "-//W3C//DTD SVG 1.1//EN" "http://www.w3.org/Graphics/SVG/1.1/DTD/svg11.dtd">

<svg version="1.1" baseProfile="full" xmlns="http://www.w3.org/2000/svg">
   <polygon id="triangle" points="0,0 0,50 50,0" fill="#009900" stroke="#004400"/>
   <script type="text/javascript">
      alert("XSS");
   </script>
</svg>
```

2. Place the file in the Android Studio project directory: /app/src/main/res/mipmap-hdpi/ic_launcher.svg



3. Zip the project directory and upload it to MobSF.

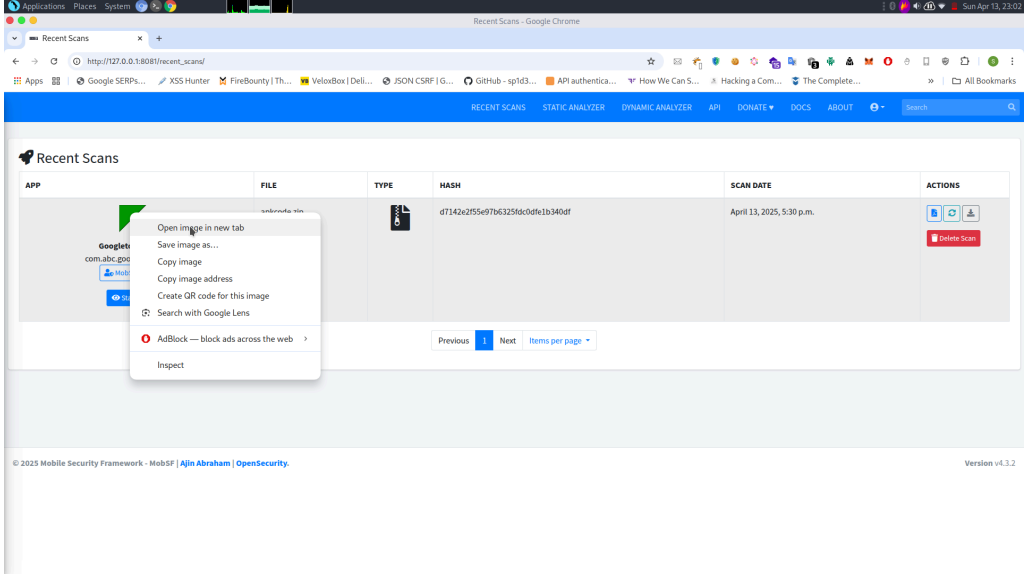


4. After the scan, navigate to the "Recent Scans" page in the MobSF web interface and click on the scan entry and open the icon file in a new browser tab.

CWE-79

Credits

ssshah2131 Reporter



5. The XSS payload is executed, confirming the vulnerability.