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

0

Valid Reported on Oct 20th 2021

Description

`Grav` is vulnerable to `XSS`. It is possible to use `&colon;` instead of `:` in `<a>` tags.

Proof of Concept

Payload:

```
<a href="javascript&colon;alert(document.domain)">CLICK HERE</a>
```

1: Edit a page with the payload (user with low privileges).
2: Check out the target page and click on `CLICK HERE`.
PoC video.

Impact

This vulnerability is capable of executing JS code.

Occurrences

Security.php L82-L125

CVE
CVE-2021-3904
(Published)

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

Severity
Medium (6.3)

Affected Version
*

Visibility
Public

Status
Fixed

Found by

Renan Rocha
@effectrenan
pro

This report was seen 551 times.

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

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

A **getgrav/grav** maintainer validated this vulnerability a year ago

Renan Rocha has been awarded the disclosure bounty ✓

The fix bounty is now up for grabs

A **getgrav/grav** maintainer marked this as fixed with commit **afc69a** a year ago

The fix bounty has been dropped ×

This vulnerability will not receive a CVE ×

Security.php#L82-L125 has been validated ✓

Jamie Slome a year ago Admin

CVE published! 🎉

Sign in to join this conversation