Server Side Template Injection in getgrav/grav

3

Valid Reported on Apr 7th 2022

Description

Grav is vulnerable to Server Side Template Injection via Twig. According to a previous vulnerability report, Twig should not render dangerous functions by default, such as `system`. PoC video.

Proof of Concept

Payload:

```
{{['cat\x20/etc/passwd']|filter('system')}}
```

With an authenticated user, access the admin panel.
Edit a page, enabling Twig in the `Advanced` tab.
Put the payload in the content.
Save and check out the post.

Impact

Remote Command execution

Occurrences

Twig.php L164-L210

References

- portswigger

CVE-2022-2073
(Published)

Vulnerability Type

CWE-94: Code Injection

Severity
Critical (9.1)

Registry
Packagist

Affected Version
Grav v1.7.32 - Admin v1.10.32

Visibility
Public

Status
Fixed

Found by

Renan Rocha

@effectrenan

pro

Fixed by

Matias Griese

@mahagr

maintainer

This report was seen 1,013 times.

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

Renan Rocha modified the report 8 months ago

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

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

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

We have sent a third and final follow up to the **getgrav/grav** team. This report is now considered stale. 7 months ago

Matias Griese modified the Severity from Critical (9.1) to Critical (9.9) 5 months ago

Matias Griese modified the Severity from Critical (9.9) to Critical (9.1) 5 months ago

Matias Griese 5 months ago Maintainer

This issue has been fixed, but we're waiting for a release before going public.

The researcher has received a minor penalty to their credibility for miscalculating the severity: -1

Matias Griese validated this vulnerability 5 months ago

Renan Rocha has been awarded the disclosure bounty ✔

The fix bounty is now up for grabs

The researcher's credibility has increased: +7

We have sent a fix follow up to the **getgrav/grav** team. We will try again in 7 days. 5 months ago

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

Matias Griese marked this as fixed in **1.7.34** with commit **9d6a2d** 5 months ago

Matias Griese has been awarded the fix bounty ✔

This vulnerability will not receive a CVE ✖

Twig.php#L164-L210 has been validated ✔

ng`bthg 14 days ago

It is still vulnerable with the payload:

```
{{['cat$IFS/etc/passwd']|map('system')|join}}
```

> Sign in to join this conversation