unprivileged user can publish a private file in silverstripe/silverstripe-assets

0

Valid Reported on Mar 27th 2022

Description

user who dont have any accesss in file can publish the file and then unauthenticated user can download that file

Proof of Concept

1. From admin account add a new user called `user-B` as `content Authors` .
Now give user-B permission in `page` section only .Dont give `files` permission .
So, user-B should not access files .

2. Now from admin account goto http://localhost/silverstripe/admin/assets/ and upload a file .
dont publish this file .
user-B should not access this file .
lets the file id is 23 .

3. Now goto user-B account and edit any page and attach a file to this page and publish that page .
Here bellow request is sent to server

```
POST /silverstripe/admin/pages/edit/EditForm/7/ HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:92.0) Gecko/20100101
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Pjax: CurrentForm,Breadcrumbs
X-Requested-With: XMLHttpRequest
Content-Length: 1925
```

Chat with us

```
Origin: http://193.37.215.120
Connection: close
Referer: http://localhost/silverstripe/admin/pages/edit/show/7
Cookie:

Title=admin-pageNew+Page&URLSegment=admin-pagenew-page&MenuTitle=admin-page
```

Here in this request just check the `Content` parameter value `<p><a href="[file_link,id=23]">sd</a><a>mjkhkh</a></p><p>` . here user-B attached a file which id is 23 .
After publish the page , above file is also published by user-B .
As user-B dont have permission in files section but still can publish that file using above request by attaching file to a page .

4. Now any external unauthenticated user visit above page will see the file link and can download the file using url like `https://localhost/silverstripe/assets/extention_brute.txt` .

So, user-B can publish a file even when he does not have permission in files .

Impact

unprivileged user can publish a file when he does not have permission in files .

Impact

publish a private file

Vulnerability Type
CWE-269: Improper Privilege Management

Severity
Medium (4.3)

Registry
Packagist

Affected Version
0.50

Visibility
Public

Status

Chat with us

Status
Fixed

Found by

ranjit-git
@ranjit-git
amateur

This report was seen 471 times.

We are processing your report and will contact the **silverstripe/silverstripe-assets** team within 24 hours. 8 months ago

ranjit-git modified the report 8 months ago

We have contacted a member of the **silverstripe/silverstripe-assets** team and are waiting to hear back 8 months ago

We have sent a follow up to the **silverstripe/silverstripe-assets** team. We will try again in 7 days. 8 months ago

We have sent a second follow up to the **silverstripe/silverstripe-assets** team. We will try again in 10 days. 8 months ago

A **silverstripe/silverstripe-assets** maintainer 8 months ago Maintainer

Thanks for submitting this, we have replicated the issue at our end

A **silverstripe/silverstripe-assets** maintainer 8 months ago Maintainer

I wasn't able to fully replicate publishing files, though there was an issue where protected images were viewable to users who should not have been able to see them

Could you please confirm if you'd liked to be acknowledged in the official disclosure? Would crediting you as follows be OK?

ranjit-git via huntr.dev

Regards
Steve Boyd
Silverstripe Product Developer

Chat with us

ranjit-git 8 months ago Researcher

@maintainer
Yes I am ok with acknowledged.

Jamie Slome 8 months ago Admin

@maintainer - is this ready to be marked as valid and fixed?

A silverstripe/silverstripe-assets maintainer 8 months ago Maintainer

We are still having internal discussions about this one as we have not fully replicated the original issue

Regards
Steve Boyd
Silverstripe Product Developer

ranjit-git 7 months ago Researcher

I will send a video poc to reproduce the bug

ranjit-git modified the report 7 months ago

We have sent a third and final follow up to the silverstripe/silverstripe-assets team. This report is now considered stale. 7 months ago

ranjit-git 7 months ago Researcher

VIDEO POC

https://drive.google.com/file/d/1X94qfBkzxlTL8pu-XUTR6s0QrsBGhlcG/view?usp=sharing

A silverstripe/silverstripe-assets maintainer 7 months ago Maintainer

On the video you provided, user11 / bug@localhost.com has the permission "E
essentially means they do have enough permissions to view and publish protected files.
Therefore the issue as originally reported where unprivileged users can published protected files

Chat with us

Therefore the issue as originally reported where unprivileged users can published protected files isn't accurate.

While investigating this issue though, there was a related issue uncovered where protected images (not files like pdfs though) are able to have be viewed in the CMS to users that shouldn't have permission to view them by sending a XHR request as described. They still cannot publish them to the public asset store though. We have developed a fix internally for this which should be released in a month or two.

We've internally assessed the CVE for this at 3.9, so I'll change the the assessment on this issue accordingly

Regards
Steve Boyd
Silverstripe Product Developer

A **silverstripe/silverstripe-assets** maintainer 7 months ago Maintainer

Sorry by CVE for this at 3.9 I meant we assessed the CVSS as a 3.9.

Regards
Steve Boyd
Silverstripe Product Developer

A **silverstripe/silverstripe-assets** maintainer 7 months ago Maintainer

This isn't letting me change the severity from 7.1 (high) to 3.9 (low) - could you please do this for me? I'm happy to confirm this once that's done

Regards
Steve Boyd
Silverstripe Product Developer

ranjit-git 7 months ago Researcher

@maintainer

```
On the video you provided, user11 / bug@localhost.com has the permission "Edit any fil
```

Chat with us

Sorry i made mistake in that video .
user11/bug@localhost.com does not need `Edit any File` file .
i forgot to revoke that permission from user11 .

You can revoke that permission and still this bug is produceble .
can you plz recalculate the CVSS score .
If severity remain same then i will change severity to your provided cvss score

ranjit-git 7 months ago Researcher

so, user11@bug@localhost.com does not have `Files section` and `Edit any file` permission .
Now user-B fully unprivileged to publish a file but using this bug he can publish

ranjit-git 7 months ago Researcher

here is the correct video poc

https://drive.google.com/file/d/1pm_qb-pa_2mrm432SrjXSH5LCDLjygEu/view?usp=sharing

Pavlos 7 months ago Admin

@maintainer sorry about the inability to assess the CVSS manually, we will deliver this functionality very soon.

In the meantime can you please tell us what vectors you used that led to a CVSS of 3.1? We will adjust it from our end :)

A silverstripe/silverstripe-assets maintainer 7 months ago Maintainer

@ranjit-git - the new video posted is literally just an admin user publishing a file with no special permissions on it.

@pavlos - https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?vector=AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C&version=3.1

Regards
Steve Boyd
Silverstripe Product Developer

ranjit-git 7 months ago

Chat with us

@maintainer
I think you did not watched the video carefully.
In this video user11 is content-author .
I think you might have confused as I recorded the video in same browser.
Acttuttly in my firefox browser I uses two account. One for admin in normal mode. Another one is content author in container-1.
You might have assumed both account as same

ranjit-git 7 months ago Researcher

Even you can reproduce the bug yourself .
Create a user with content-author permision and then revoke file section permission and revoke edit-any-file permiision.
And this user can publish file using this bug
.

ranjit-git 7 months ago Researcher

Just give me another chance I will properly make a video with written.
Within hour I will upload a video

ranjit-git 7 months ago Researcher

VIDEO POC

https://drive.google.com/file/d/1uiMYZYq1XOquuWQLivLUV2a-KMS_1yzx/view

my steps

admin add a user in content-author group .

revoke bellow permission for content-author group
File section permission and Edit-Any-File permiision

goto content-author user account and publish the file like in my video

Plz let me know your file decision and final CVSS score .

Chat with us

ranjit-git modified the report 7 months ago

ranjit-git 7 months ago Researcher

@maintainer
i have adjusted your provided cvss score https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?vector=AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C&version=3.1
Plz lt me know if any issue

A silverstripe/silverstripe-assets maintainer validated this vulnerability 7 months ago

ranjit-git 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 silverstripe/silverstripe-assets team. We will try again in 7 days. 7 months ago

We have sent a second fix follow up to the silverstripe/silverstripe-assets team. We will try again in 10 days. 7 months ago

We have sent a third and final fix follow up to the silverstripe/silverstripe-assets team. This report is now considered stale. 6 months ago

A silverstripe/silverstripe-assets maintainer 5 months ago Maintainer

@Pavlos

I'd like to mark as fixed, though the fix is in silverstripe/assets, not silverstripe/framework

Fixed in version:
1.10.1

SHA:
5f6a73b010c01587ffbfb954441f6b7cbb54e767

Who should get rewarded for the patch:
Nobody

Jamie Slome marked this as fixed in 1.10.1 with commit 5f6a73 5 months ag

The fix bounty has been dropped ✖

Chat with us

This vulnerability will not receive a CVE ✖

Jamie Slome 5 months ago Admin

Sorted 👍

Sign in to join this conversation

2022 © 418sec

Chat with us