zvory / csv-safe Public

Code Issues Pull requests 1 Actions Projects Security ···

New issue Jump to bottom

Older versions of CSV-Safe gem doesn't filter out special characters which could trigger CSV Injection. (< 3.0.0) [CVE-2022-28481] #7

Closed danishtariqq opened this issue on Mar 10 · 7 comments

danishtariqq commented on Mar 10 • edited Contributor

Older versions of CSV-Safe gem doesn't filter out special characters which could trigger CSV Injection. (< 3.0.0)

Vulnerability Type
CSV Injection

Product
csv-safe

Affected Product Code Base
CSV-safe - <3.0.0 are effected

Affected Component
Sanitization of CSV Injection vectors.

Attack Type
Remote

Attack Vector
%0A-3+3+cmd|' /C calc'!D2 could be used to bypass CSV injection sanitizations in older versions.

Credits
Danish Tariq
Ali Hassan Ghori
Hassan Khan Yusufzai

Fixed by
Gabriel Rios - #8

References
https://github.com/zvory/csv-safe
#8
https://hackerone.com/reports/223999
WeblateOrg/weblate@ `d9e136f`
https://bugzilla.mozilla.org/show_bug.cgi?id=1259881

👍 1 🎉 1 ❤️ 1 🚀 1

gabrielrios mentioned this issue on Mar 16

Prefix starting with '%' #8

Merged

zvory commented on Mar 16 Owner

Thank you.

danishtariqq commented on Mar 23 Contributor Author

#8

danishtariqq closed this as completed on Mar 23

danishtariqq commented on Mar 24 Contributor Author

@zvory Can we claim CVE for this? i.e. Older version was not secured properly to filtrate enough characters against CSV Injection so was not fully securing and thus could be a cause of vulnerability in applications using older versions of csv-safe gem.

Steps needs to be done could be simply putting it in the Security advisory of your repository and adding details on why the newer version was created.

zvory commented on Mar 24 Owner

@danishtariqq Could you put up a PR?

danishtariqq commented on Mar 25 Contributor Author

> @danishtariqq Could you put up a PR?

#8 @zvory

zvory commented on Mar 27 Owner

@danishtariqq Oh sorry I meant for the CVE. I assumed that went into the repo. If it doesn't, feel free to make one! Sounds like a good idea.

danishtariqq changed the title ~~More special characters needs to be filtered out for a better security~~ **Older versions of CSV-Safe gem doesn't filter out special characters which could trigger CSV Injection. (> 3.0.0)** on Mar 28

danishtariqq changed the title ~~Older versions of CSV-Safe gem doesn't filter out special characters which could trigger CSV Injection. (> 3.0.0)~~ **Older versions of CSV-Safe gem doesn't filter out special characters which could trigger CSV Injection. (< 3.0.0)** on Mar 28

danishtariqq commented on Mar 28 Contributor Author

@zvory - #9

danishtariqq changed the title ~~Older versions of CSV-Safe gem doesn't filter out special characters which could trigger CSV Injection. (< 3.0.0)~~ **Older versions of CSV-Safe gem doesn't filter out special characters which could trigger CSV Injection. (< 3.0.0) [CVE-2022-28481]** on May 2

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants