Path Traversal in plankanban/planka

0

Valid Reported on Aug 1st 2022

Description

Via the `/attachments/:id/download/thumbnails/:filename` endpoint, an authenticated user can access any arbitrary file in the system through a path traversal vulnerability in the `filename` parameter.

The `filename` parameter is not sanitized and its used to craft the path of the target file. Using the encoded value of the slash character `%2F` allows to traverse to any directory the attacker wants, and read any file.

Proof of Concept

1 - Log in and get a `id` of a project that has at least one image. If no image is available upload a new one.
2 - Sending the following request allows to read the contents of the `/proc/self/environ` file.

```
GET http://localhost:3000/attachments/<project-id>/download/thumbnails/..%2
```

Impact

With this vulnerability an attacker can read many sensitive files like configura
`/proc/self/environ` file, that contains the environment variable used by the web server that

includes database credentials. If the web server user is root, an attacker will be able to read any file in the system.

Occurrences

JS download-thumbnail.js L57

CVE
CVE-2022-2653
(Published)

Vulnerability Type
CWE-22: Path Traversal

Severity
High (7.1)

Registry
Npm

Affected Version
1.5.0

Visibility
Public

Status
Fixed

Found by

vultza
@vultza
legend

This report was seen 696 times.

We are processing your report and will contact the **plankanban/planka** team within 24 hours.
4 months ago

We created a **GitHub Issue** asking the maintainers to create a `SECURITY.md`

Chat with us

We have contacted a member of the **plankanban/planka** team and are waiting to hear back

We have contacted a member of the plankanban/planka team and are waiting to hear back
4 months ago

Maksim Eltyshev validated this vulnerability 4 months ago

vultza has been awarded the disclosure bounty ✔

The fix bounty is now up for grabs

The researcher's credibility has increased: +7

Maksim Eltyshev marked this as fixed in 1.5.1 with commit ac1df5 4 months ago

The fix bounty has been dropped ✖

This vulnerability will not receive a CVE ✖

download-thumbnail.js#L57 has been validated ✔

Maksim Eltyshev gave praise 4 months ago

Thank you so much for reporting this issue!

The researcher's credibility has slightly increased as a result of the maintainer's thanks: +1

amammad 4 months ago

I want to say that you can request a CVE here from the Huntr team!

Jamie Slome 4 months ago Admin

Sorted :)

vultza 4 months ago Researcher

Thanks guys, appreciated.

Sign in to join this conversation

Sign in to join this conversation