Unhandled exception on illegal filename_disk value

Moderate **rijkvanzanten** published **GHSA-77qm-wvqq-fg79** on Aug 19

Package

directus (npm)

Affected versions	Patched versions
< 9.15.0	9.15.0

Description

Impact

What kind of vulnerability is it? Who is impacted?

The Directus process can be aborted by having an authorized user update the `filename_disk` value to a folder and accessing that file through the `/assets` endpoint.

Patches

Has the problem been patched? What versions should users upgrade to?

The vulnerability is patched and released in v9.15.0.

Workarounds

Is there a way for users to fix or remediate the vulnerability without upgrading?

You can prevent this problem by making sure no (untrusted) non-admin users have permissions to update the `filename_disk` field on `directus_files`.

For more information

If you have any questions or comments about this advisory:

- Open a Discussion in directus/directus

- Email us at security@directus.io

Credits

This vulnerability was first discovered and reported by Witold Gorecki.

Severity

Moderate 6.5 / 10

CVSS base metrics

Attack vector	Network
Attack complexity	Low
Privileges required	Low
User interaction	None
Scope	Unchanged
Confidentiality	None
Integrity	None
Availability	High

CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H

CVE ID

CVE-2022-36031

Weaknesses

No CWEs

Credits

wgorecki