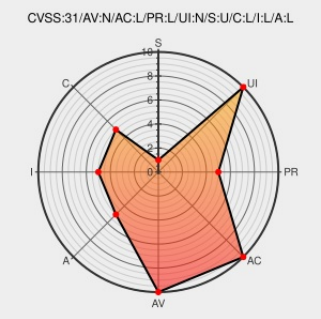
CVE-2022-3939

Published on: Not Yet Published

Last Modified on: 11/15/2022 09:30:00 PM UTC

CVE-2022-3939

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Ferry from Ferry Project contain the following vulnerability:

A vulnerability, which was classified as critical, has been found in lanyulei ferry. Affected by this issue is some unknown functionality of the file apis/public/file.go of the component API. The manipulation of the argument file leads to path traversal. The attack may be launched remotely. VDB-213446 is the identifier assigned to this vulnerability.

CVE-2022-3939 has been assigned by cna@vuldb.com to track the vulnerability - currently rated as CRITICAL severity.

Affected Vendor/Software: **lanyulei** - **ferry** version **n/a**

CVSS3 Score: 9.8 - CRITICAL

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	HIGH	HIGH

CVE References

Description	Tags	Link
CVE-2022-3939 | lanyulei ferry API file.go path traversal	vuldb.com text/html	MISC vuldb.com/?id.213446

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Ferry Project	Ferry	-	All	All	All

cpe:2.3:a:ferry_project:ferry:-:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
/r/netcve	CVE-2022-3939	2022-11-11 08:38:34

← Previous ID

Next ID→