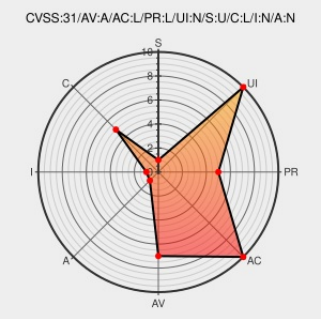
CVE-2022-3940

Published on: Not Yet Published

Last Modified on: 11/15/2022 09:33:00 PM UTC

CVE-2022-3940

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 problematic, was found in lanyulei ferry. This affects an unknown part of the file apis/process/task.go. The manipulation of the argument file_name leads to path traversal. The associated identifier of this vulnerability is VDB-213447.

CVE-2022-3940 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-2022-3940 | lanyulei ferry task.go path traversal	vuldb.com text/html	MISC vuldb.com/?id.213447

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)
@CVEreport	CVE-2022-3940 : A vulnerability, which was classified as problematic, was found in lanyulei ferry. This affects an… twitter.com/i/web/status/1…	2022-11-11 07:16:20
/r/netcve	CVE-2022-3940	2022-11-11 08:38:34

← Previous ID

Next ID→