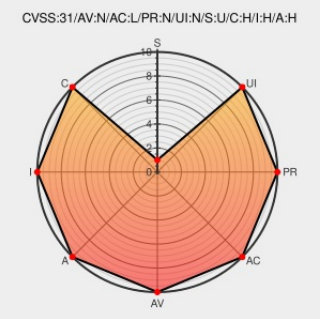
CVE-2022-26245

Published on: Not Yet Published

Last Modified on: 04/05/2022 01:21:00 PM UTC

CVE-2022-26245

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



Certain versions of Falcon-plus from Open-falcon contain the following vulnerability:

Falcon-plus v0.3 was discovered to contain a SQL injection vulnerability via the parameter grpName in /config/service/host.go.

CVE-2022-26245 has been assigned by cve@mitre.org to track the vulnerability - currently rated as CRITICAL severity.

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

CVSS2 Score: 7.5 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
report sqlinjection vulnerability · Issue #951 · open-falcon/falcon-plus · GitHub	github.com text/html	MISC github.com/open-falcon/falcon-plus/issues/951

are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Open-falcon	Falcon-plus	0.3	All	All	All

cpe:2.3:a:open-falcon:falcon-plus:0.3:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@Robo_Alerts	Potentially Critical CVE Detected! CVE-2022-26245 Falcon-plus v0.3 was discovered to contain a SQL injection vulner… twitter.com/i/web/status/1…	2022-03-27 14:56:01
/r/netcve	CVE-2022-26245	2022-03-27 14:38:05

← Previous ID

Next ID→

CVE.report and Source URL Uptime Status status.cve.report