



CVE-2022-24849

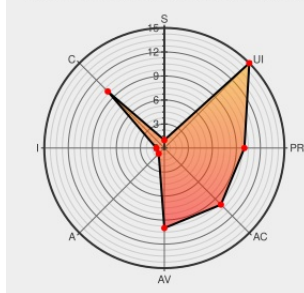
Published on: Not Yet Published

Last Modified on: 04/22/2022 07:42:00 PM UTC

CVE-2022-24849 - advisory for GHSA-frxg-hf44-q765

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#)

CVSS:31/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N



Certain versions of [Discatsharp](#) from [Aitsys](#) contain the following vulnerability:

DisCatSharp is a Discord API wrapper for .NET. Users of versions 9.8.5, 9.8.6, 9.9.0 and previously published prereleases of 10.0.0 who have used either one of the two

``RequireDisCatSharpDeveloperAttribute`s` or the

``BaseDiscordClient.LibraryDeveloperTeam`` have potentially had their

bot token sent to a web server not affiliated with Discord. This server is owned and operated by DisCatSharp's development team. The tokens were not logged, yet it is still advisable to reset the tokens of potentially affected bots. 9.9.1 has been released to patch the issue for the current stable release and the current 10.0.0 prereleases are also no longer affected. Users unable to upgrade should remove all uses of the two

``RequireDisCatSharpDeveloperAttribute`s` and all direct calls to ``BaseDiscordClient.LibraryDeveloperTeam``.

CVE-2022-24849 has been assigned by [security-advisories@github.com](#) to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: **Aiko-IT-Systems - DisCatSharp** version **>= 9.8.5, < 9.9.1**

CVSS3 Score: **6.5 - MEDIUM**

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

CVSS2 Score: **4.3 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE

Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	NONE	NONE

CVE References

Description	Tags	Link
Contact to DisCatSharp-owned server using authenticated client · Advisory · Aiko-IT-Systems/DisCatSharp · GitHub	github.com text/html	CONFIRM github.com/Aiko-IT-Systems/DisCatSharp/security/advisories/GHSA-frxg-hf44-q765

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that 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	Aitsys	Discatsharp	All	All	All	All

```
cpe:2.3:a:aitsys:discatsharp:*:*:*:*:*:*:
```

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2022-24849 : DisCatSharp is a Discord API wrapper for .NET. Users of versions 9.8.5, 9.8.6, 9.9.0 and previous... twitter.com/i/web/status/1...	2022-04-14 21:32:42
/r/netcve	CVE-2022-24849	2022-04-14 22:38:15

[← Previous ID](#)
[Next ID →](#)