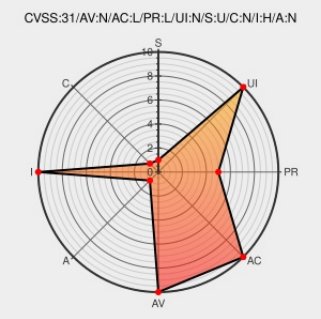
CVE-2023-22452

Published on: Not Yet Published

Last Modified on: 01/09/2023 07:53:00 PM UTC

CVE-2023-22452 - advisory for GHSA-73j8-xrcr-q6j7

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



Certain versions of Kenny2automate from Kenny2automate Project contain the following vulnerability:

kenny2automate is a Discord bot. In the web interface for server settings, form elements were generated with Discord channel IDs as part of input names. Prior to commit a947d7c, no validation was performed to ensure that the channel IDs submitted actually belonged to the server being configured. Thus anyone who has access to the channel ID they wish to change settings for and the server settings panel for any server could change settings for the requested channel no matter which server it belonged to. Commit a947d7c resolves the issue and has been deployed to the official instance of the bot. The only workaround that exists is to disable the web config entirely by changing it to run on localhost. Note that a workaround is only necessary for those who run their own instance of the bot.

CVE-2023-22452 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **Kenny2github** - **kenny2automate** version **= < a947d7c**

CVSS3 Score: 6.5 - MEDIUM

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

CVE References

Description	Tags	Link
Improper Input Validation in kenny2automate · Advisory · Kenny2github/kenny2automate · GitHub	github.com text/html	MISC github.com/Kenny2github/kenny2automate/security/advisories/GHSA-73j

SECURITY: Prevent changing other servers' settings · Kenny2github/kenny2automate@a947d7c · GitHub	github.com text/html	MISC github.com/Kenny2github/kenny2automate/commit/a947d7ce408687b587c7e6dfd6

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	Kenny2automate Project	Kenny2automate	All	All	All	All

cpe:2.3:a:kenny2automate_project:kenny2automate:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2023-22452 : kenny2automate is a Discord bot. In the web interface for server settings, form elements were gene… twitter.com/i/web/status/1…	2023-01-02 20:02:15

← Previous ID Next ID→