Directory Traversal in AiScript via `Mk:api`

Moderate **syuilo** published **GHSA-gmq6-738q-vjp2** yesterday

Package	Affected versions	Patched versions
Misskey	>=12.31.0	None

Description

Summary

Missing validation in `Mk:api` allows malicious AiScript code to access additional endpoints that it isn't designed to have access to.

Details

The missing validation allows malicious AiScript code to prefix a URL with `../` to step out of the `/api` directory, thereby being able to make requests to other endpoints, such as `/files`, `/url`, and `/proxy`.

PoC

```
// This doesn't actually do anything, but it shows that it's mal th
// request with directory traversal if you check devtools
Mk:api('../proxy/avatar.webp?url=https%3A%2F%2Finsertdomain.name%2Fas
```

Impact

Hard to say how much a malicious actor could do with this, given that they already have access to the other API endpoints, but its better to be safe.

Severity

Moderate 5.4 / 10

CVSS v3 base metrics

Attack vector	Network
Attack complexity	High
Privileges required	Low
User interaction	Required
Scope	Unchanged
Confidentiality	Low
Integrity	High
Availability	None

Learn more about base metrics

CVSS:3.1/AV:N/AC:H/PR:L/UI:R/S:U/C:L/I:H/A:N

CVE ID

CVE-2025-46559

Weaknesses

No CWEs

Credits

warriordog Finder