Security: Implement SSRF and Rate Limit Protections #659

Closed **Dave-gilmore-aus** wants to merge 1 commit into `danielmiessler:main` from `Dave-gilmore-aus:fix/voiceserver-…`

Conversation 1 Commits 1 Checks 0 Files changed 1

Dave-gilmore-aus commented on Feb 14

Description
This PR implements security hardening for the VoiceServer. It specifically addresses SSRF risks and rate-limit bypasses identified during a security audit.

Changes
SSRF Protection: Added a validateUrl helper to block requests to internal IP ranges (localhost, private LANs, and cloud metadata services) before fetch calls.

Rate Limit Security: Modified IP detection to use server.requestIP(req) instead of the untrusted x-forwarded-for header to prevent spoofing.

These changes align with the "Defense Strategies" outlined in the project's SECURITY.md.

`Security: implement SSRF protection and secure rate limiting` `14322e8`

kaimagnus commented on Feb 15 Collaborator

Thank you for the SSRF and rate limiting protections, **@Dave-gilmore-aus**! Important security hardening for the voice server — the URL validation blocking internal IPs is well-implemented.

The target path (`Packs/pai-voice-system/`) no longer exists in v3.0. Closing as the paths don't match. We'll apply these security patterns to the v3.0 voice server. Great security work!

kaimagnus closed this on Feb 15

Sign up for free **to join this conversation on GitHub**. Already have an account? Sign in to comment

Reviewers

No reviews

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

Successfully merging this pull request may close these issues.

None yet

2 participants