


RocketChat / Rocket.Chat Public[Code](#) [Issues](#) 2.4k [Pull requests](#) 1.3k [Discussions](#) [Actions](#) [Projects](#)

fix: add validation for SAML SLO redirect URLs #38994

Merged [julio-rocketchat](#) merged 9 commits into [develop](#) from [saml-redirect-validation](#) 
3 weeks ago

[Conversation](#) 19 [Commits](#) 9 [Checks](#) 44 [Files changed](#) 2



[yasnagat](#) commented on [Feb 24](#) • edited by [coderabbitai](#) bot 

Member

Proposed changes (including videos or screenshots)

The SAML Single Logout (SLO) redirect functionality was vulnerable to open redirect attacks. Users could be redirected to arbitrary external URLs by manipulating the redirect query parameter, potentially leading to phishing attacks or credential theft.

This happened because the `processSLORedirectAction` function directly used the user-supplied redirect parameter without validation, allowing attackers to craft malicious URLs like:

```
/_saml/sloRedirect/saml-test/?redirect=https://malicious-site.com
```

This PR:

- Validates redirect URLs against the configured IDP Single Logout Service endpoint;
- Implements origin and pathname matching to ensure redirects only go to the configured IDP.

Issue(s)

[VLN-153](#), [VLN-165](#)

Steps to test or reproduce

N/A

Further comments

N/A

Summary by CodeRabbit

• Bug Fixes

- Strengthened SAML Single Logout (SLO) redirect validation to block malformed or unauthorized redirect URLs.
- Added strict presence, format and URL parsing checks for redirect parameters with clear error responses (400/403/500) for invalid input.
- Enforced origin and normalized path matching between configured IdP SLO and requested redirect; redirects now use the validated URL.

• Chores

- Added a changeset documenting the SAML redirect validation patch.



[fix: add validation for SAML SLO redirect URLs](#)

✖ [f574d8c](#)

dionisio-bot bot commented on [Feb 24](#) • edited ▾

Contributor

Looks like this PR is ready to merge! 🎉
If you have any trouble, please check the [PR guidelines](#)

changeset-bot bot commented on [Feb 24](#) • edited ▾

Changeset detected

Latest commit: [6b923a5](#)

The changes in this PR will be included in the next version bump.

► This PR includes changesets to release 41 packages

Not sure what this means? [Click here to learn what changesets are.](#)

[Click here if you're a maintainer who wants to add another changeset to this PR](#)

coderrabbitai bot commented on [Feb 24](#) • edited ▾

Contributor

 Note

Reviews paused



It looks like this branch is under active development. To avoid overwhelming you with review comments due to an influx of new commits, CodeRabbit has automatically paused this review. You can configure this behavior by changing the

`reviews.auto_review.auto_pause_after_reviewed_commits` setting.

Use the following commands to manage reviews:

- `@coderabbitai resume` to resume automatic reviews.
- `@coderabbitai review` to trigger a single review.

Use the checkboxes below for quick actions:

-  Resume reviews
-  Trigger review

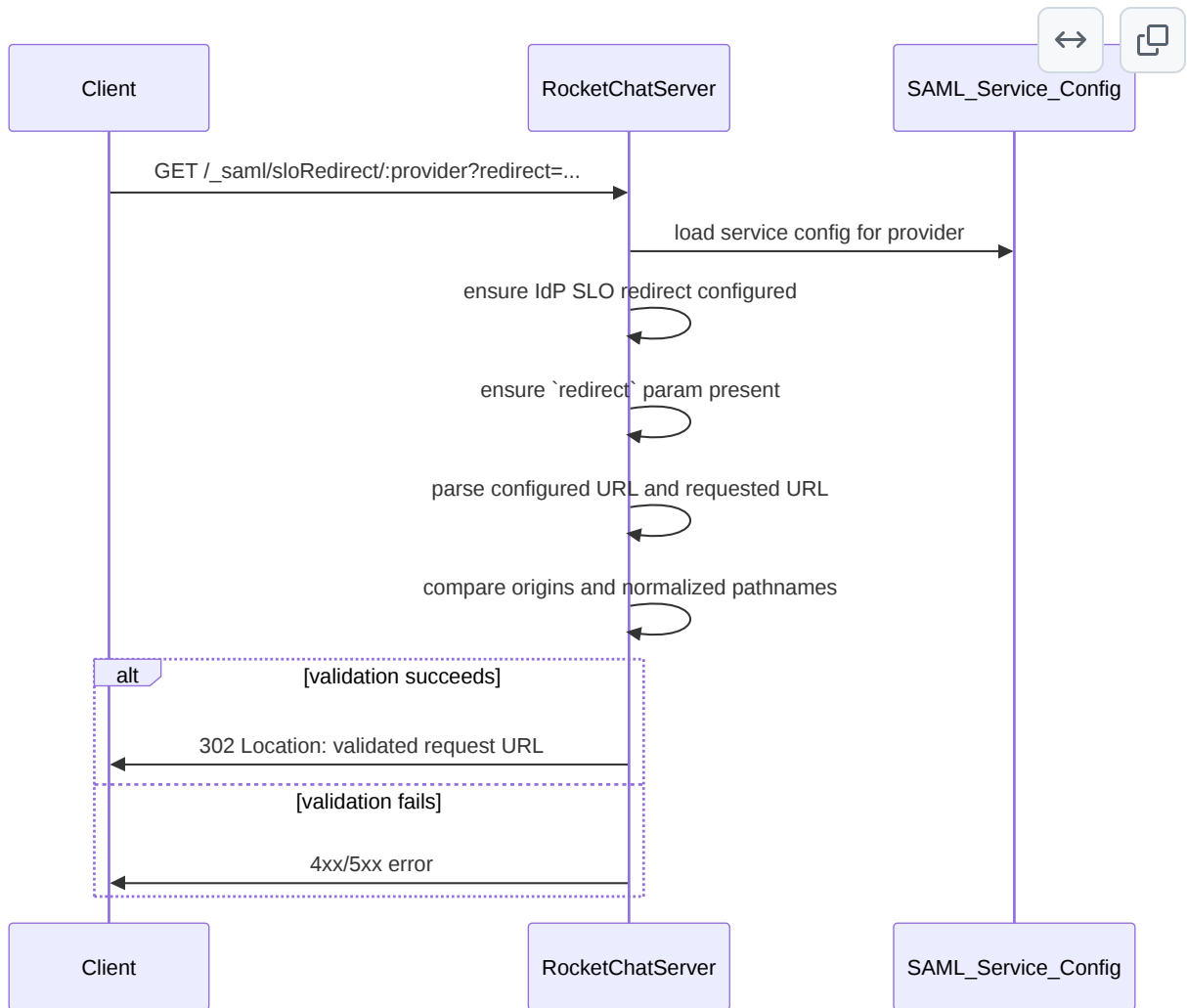
Walkthrough

SAML SLO redirect handling now requires the SAML service, validates the configured IdP SLO URL and the user-provided `redirect` parameter, parses both URLs, enforces origin and normalized pathname equality, and redirects to the validated request URL or returns 4xx/5xx on failure.

Changes

Cohort / File(s)	Summary
SAML SLO Redirect Validation <code>apps/meteor/app/meteor-accounts-saml/server/lib/SAML.ts</code>	<code>processSLORedirectAction</code> signature updated to accept <code>service</code> . Added checks: require configured IdP SLO redirect (500), require user <code>redirect</code> param (400), parse/validate both URLs (400 on parse failure), enforce origin match and normalized pathname equality (403 on mismatch), and set <code>Location</code> to the validated request URL.
Changeset <code>.changeset/metal-rice-retire.md</code>	Adds a changeset entry documenting the SAML redirect validation change (patch).

Sequence Diagram(s)



Estimated code review effort

🎯 3 (Moderate) | ⌚ ~20 minutes

Suggested labels

type: bug

▶ 🚦 Pre-merge checks | ✅ 5

▶ 📝 Coding Plan

Thanks for using [CodeRabbit!](#) It's free for OSS, and your support helps us grow. If you like it, consider giving us a shout-out.

▶ Share

Comment `@coderabbitai help` to get the list of available commands and usage tips.

Tip

▶ CodeRabbit can approve the review once all CodeRabbit's comments are resolved.



coderabbitai bot reviewed [on Feb 24](#)

[View reviewed changes](#)



coderabbitai bot left a comment

Contributor

Actionable comments posted: 3

▶ Prompt for all review comments with AI agents

▶ Review info

▶ Review details

apps/meteor/app/meteor-accounts-saml/server/lib/SAML.ts

Show resolved

apps/meteor/app/meteor-accounts-saml/server/lib/SAML.ts

Show resolved

apps/meteor/app/meteor-accounts-saml/server/lib/SAML.ts

Outdated

Show resolved

codecov bot commented [on Feb 24](#) • edited ▾

Codecov Report

✓ All modified and coverable lines are covered by tests.

✓ Project coverage is 70.49%. Comparing base ([8b32bc9](#)) to head ([6b923a5](#)).


⚠ Report is 25 commits behind head on develop.

- ▶ Additional details and impacted files
- ▶ 🚀 New features to boost your workflow:

📄 **yasnagat** added 2 commits [2 months ago](#)


🔗  [Normalize path comparison for redirect validation](#) ✖ [fd4998d](#)

🔗  [Merge branch 'develop' into saml-redirect-validation](#) ✖ [8411cf9](#)

🏷️  **ggazzo** added the area: authentication label [on Feb 27](#)





👁️  **yasnagat** marked this pull request as ready for review [last month](#)


🏷️  **coderrabbitai** bot added type: bug and removed area: authentication labels [on Mar 2](#)

👁️  **coderrabbitai** bot reviewed [on Mar 2](#)


[View reviewed changes](#)

 **coderrabbitai** bot left a comment Contributor

- ▶  Duplicate comments (2)
 - ▶  Prompt for all review comments with AI agents
-
- ▶  Review info
 - ▶  Review details

👁️  **cubic-dev-ai** bot reviewed [on Mar 2](#)

[View reviewed changes](#)

 **cubic-dev-ai** bot left a comment Contributor

1 issue found across 1 file

- ▶ Prompt for AI agents (unresolved issues)

Reply with feedback, questions, or to request a fix. Tag `@cubic-dev-ai` to re-run a review.

apps/meteor/app/meteor-accounts-saml/server/lib/SAML.ts

Show resolved



pierre-lehnen-rc requested changes on Mar 2

View reviewed changes

apps/meteor/app/meteor-accounts-saml/server/lib/SAML.ts

Outdated

Show resolved



Update apps/meteor/app/meteor-accounts-saml/server/lib/SAML.ts



6843866



coderabbitai bot

added

area: authentication

and removed

type: bug

labels on Mar 3



coderabbitai bot

reviewed

on Mar 3

View reviewed changes



coderabbitai bot

left a comment

Contributor

Actionable comments posted: 1

- ▶ Prompt for all review comments with AI agents

- ▶ Review info

- ▶ Review details

apps/meteor/app/meteor-accounts-saml/server/lib/SAML.ts

Show resolved



KevLehman requested changes on Mar 3

View reviewed changes



KevLehman left a comment

Member

pls add a changeset



`add changeset file`

✖ [568e6c3](#)



coderabbitai (bot) added `type: bug` and removed `area: authentication` labels [on Mar 4](#)



pierre-lehnen-rc previously approved these changes [on Mar 5](#)

[View reviewed changes](#)



pierre-lehnen-rc left a comment

Contributor

Not sure but maybe we should redirect to home in case of error, as the client is not expecting this redirect to ever fail and won't be able to recover from it (though there should also not be any errors on normal usage)



1



KevLehman previously approved these changes [on Mar 5](#)

[View reviewed changes](#)



yasnagat added this to the **8.3.0** milestone [on Mar 5](#)



julio-rocketchat reviewed [last month](#)

[View reviewed changes](#)

`apps/meteor/app/meteor-accounts-saml/server/lib/SAML.ts`

Outdated



Show resolved





























Merge branch '`develop`' into `saml-redirect-validation`

✖ [@e154f3](#)



coderabbitai (bot) added `area: authentication` and removed `type: bug` labels [last month](#)

-   [Update apps/meteor/app/meteor-accounts-saml/server/lib/SAML.ts](#) ✖ [3346067](#)
-   **julio-rocketchat** dismissed stale reviews from **KevLehman** and **pierre-lehnen-rc** via [3346067](#) last month
-   [Merge branch 'develop' into saml-redirect-validation](#) ✔ [7dd041a](#)
-   **julio-rocketchat** approved these changes last month
[View reviewed changes](#)
-   **julio-rocketchat** added the stat: QA assured label last month
-   **dionisio-bot** bot added the stat: ready to merge label last month
-   **dionisio-bot** bot enabled auto-merge last month
-   **coderrabbitai** bot added type: bug and removed area: authentication labels last month
-   **dionisio-bot** bot added this pull request to the [merge queue](#) last month
-   **github-merge-queue** bot removed this pull request from the [merge queue](#) due to failed status checks last month View details
-   [Merge branch 'develop' into saml-redirect-validation](#) ✔ [6b923a5](#)
-   **dionisio-bot** bot enabled auto-merge last month
-   **dionisio-bot** bot added this pull request to the [merge queue](#) last month



KevLehman approved these changes [last month](#)

[View reviewed changes](#)



github-merge-queue bot removed this pull request from the [merge queue](#) due to failed status checks [last month](#)

[View details](#)



julio-rocketchat added this pull request to the [merge queue](#) [3 weeks ago](#)



julio-rocketchat modified the milestones: **8.3.0**, **8.4.0** [3 weeks ago](#)



Merged via the queue into `develop` with commit **d12b53c** [3 weeks ago](#)
46 checks passed

[View details](#)



julio-rocketchat deleted the `saml-redirect-validation` branch [3 weeks ago](#)

[Sign up for free](#) to join this conversation on GitHub. Already have an account? [Sign in to comment](#)

Reviewers



coderabbitai[bot]



cubic-dev-ai[bot]



KevLehman



julio-rocketchat



pierre-lehnen-rc



Assignees

No one assigned

Labels

stat: QA assured

stat: ready to merge

type: bug

Projects

None yet

Milestone



8.4.0

Development

Successfully merging this pull request may close these issues.

None yet

5 participants

