

fix: block internal REST targets by default #18236

Merged melohagan merged 15 commits into master from fix/ssrf-rest on Mar 13

Conversation Commits 15 Checks Files changed

melohagan commented on Mar 10 • edited by cubic-dev-ai Bot Collaborator

Description

Fix the REST datasource SSRF protection so it blocks internal and link-local IP ranges by default, even when BLACKLIST_IPS is unset. This closes the insecure default described in <https://github.com/Budibase/vulns/issues/26>.

Addresses

- <https://github.com/Budibase/vulns/issues/26>

Launchcontrol

Block REST datasource requests to internal network ranges by default so self-hosted instances are protected without extra blacklist configuration.

Summary by cubic

Block REST datasource requests to internal, loopback, and link-local IPs by default, even when BLACKLIST_IPS is unset. DNS lookup or URL parsing failures now fail closed; malformed URLs are rejected, and bracketed IPv6 hosts are parsed safely, closing <https://github.com/Budibase/vulns/issues/26>.



- **Bug Fixes**
 - Added a default CIDR blacklist (IPv4/IPv6: 127.0.0.0/8, 10/8, 172.16/12, 192.168/16, 169.254/16, 0.0.0.0/8, ::1/128, fc00::/7, fe80::/10).

- Switched to `net.BlockList` with IPv4/IPv6 + CIDR support; merges `BLACKLIST_IPS`, resolves domain entries to IPs, and checks subnets.
- Improved parsing and DNS handling: normalizes bracketed IPv6 hosts; DNS or URL parsing errors now block (fail-closed); malformed URLs are blocked.
- Tightened CIDR validation: ignore invalid prefixes, multiple slashes, or non-numeric masks; only in-range numeric masks are accepted.

Written for commit [473bc2c](#). Summary will update on new commits.


  [Fix default REST SSRF blacklist](#) 62f50d9

  **github-actions** Bot added the `size/m` label [on Mar 10](#)

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

  **melohagan** requested a review from **a team** as a [code owner](#) [last month](#)

  **melohagan** requested review from **adrinr** and removed request for **a team** [last month](#)

 **cubic-dev-ai** Bot reviewed [on Mar 10](#)

[View reviewed changes](#)

 **cubic-dev-ai** Bot left a comment

Contributor

2 issues found across 3 files

Confidence score: **2/5**

- There is a high-confidence security concern in `packages/backend-core/src/blacklist/blacklist.ts`: fail-open handling returns `false` on parse/lookup errors, which could let crafted URLs bypass blacklist checks (SSRF risk).
- This is the main reason for the lower score—severity is high (7/10) with strong confidence (8/10), so merge risk is elevated until fail-closed behavior is enforced.
- The test issue in `packages/backend-core/src/blacklist/tests/blacklist.spec.ts` is lower risk (4/10): using `env._set` directly can leak environment state between tests, but this is more of a reliability/maintainability fix than a blocker.
- Pay close attention to `packages/backend-core/src/blacklist/blacklist.ts`, `packages/backend-core/src/blacklist/tests/blacklist.spec.ts` - SSRF bypass risk from fail-open logic and test env

leakage from direct mutation.

► Prompt for AI agents (unresolved issues)

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

> packages/backend-core/src/blacklist/blacklist.ts Outdated Show resolved

> packages/backend-core/src/blacklist/tests/blacklist.spec.ts Outdated Show resolved

👁 chatgpt-codex-connector Bot reviewed on Mar 10

View reviewed changes

🌀 chatgpt-codex-connector Bot left a comment

💡 Codex Review

Here are some automated review suggestions for this pull request.

Reviewed commit: 62f50d9779

► ⓘ About Codex in GitHub

> packages/backend-core/src/blacklist/blacklist.ts Outdated Show resolved

✅ calexiou approved these changes on Mar 10









View reviewed changes


👤 calexiou left a comment Contributor

thanks @melohagan

👍 1

📁 melohagan and others added 4 commits last month

-   [Fix blacklist fail-open lookup handling](#) 9b2ede8
-   [Merge branch 'master' into fix/ssrf-rest](#) 63d6b75
-   [lint](#) e911e45
-   [Fix malformed blacklist CIDR parsing](#) 82c2c8a

 **cubic-dev-ai** Bot reviewed [on Mar 10](#)

[View reviewed changes](#)



cubic-dev-ai Bot left a comment

Contributor

1 issue found across 2 files (changes from recent commits).









▶ [Prompt for AI agents \(unresolved issues\)](#)

Reply with feedback, questions, or to request a fix. Tag [@cubic-dev-ai](#) to re-run a review.

> `packages/backend-core/src/blacklist/blacklist.ts`

 Show resolved

 **melohagan** added 4 commits [last month](#)

-   [Fix blacklist CIDR validation](#) 633f828
-   [Fix OAuth2 automation blacklist tests](#) ae71deb
-   [Fix blacklist DNS lookup handling](#) a06a1b1
-   [Revert "Fix OAuth2 automation blacklist tests"](#) 30768d6

 **cubic-dev-ai** Bot reviewed [on Mar 10](#)

[View reviewed changes](#)



cubic-dev-ai Bot left a comment

Contributor

1 issue found across 3 files (changes from recent commits).

▶ [Prompt for AI agents \(unresolved issues\)](#)

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

> packages/backend-core/src/blacklist/blacklist.ts Outdated Show resolved

Revert "Fix blacklist DNS lookup handling" ... 3050d0f

melohagan added the do not merge label on Mar 10

Fix fail-closed blacklist test fixtures 05c6695

melohagan removed the do not merge label on Mar 12

melohagan added 4 commits last month

Merge branch 'master' into fix/ssrf-rest 1ec5974

Merge branch 'master' into fix/ssrf-rest 09871de

Merge branch 'master' into fix/ssrf-rest e7a9212

Merge branch 'master' into fix/ssrf-rest 473bc2c

melohagan enabled auto-merge last month

melohagan merged commit **5b0fe83** into master on Mar 13 31 checks passed View details

melohagan deleted the fix/ssrf-rest branch last month

github-actions Bot locked and limited conversation to collaborators on Mar 13

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

Reviewers

-  cubic-dev-ai[bot] 
 -  chatgpt-codex-connector[bot] 
 -  calexiou 
 -  adrinr  
-

Assignees

No one assigned

Labels

size/m

Projects

None yet

Milestone

No milestone

Development

Successfully merging this pull request may close these issues.

None yet

2 participants

