New issue

Missing Authentication on Administrative API Endpoints Leads to Full System Compromise in 9Router #431

Closed

deepcat1337 opened 2 weeks ago

A critical broken access control vulnerability exists in 9Router due to improper enforcement of authentication boundaries. While access control is applied to `/dashboard` routes via middleware, multiple sensitive `/api/*` endpoints lack server-side authentication and authorization checks.

As a result, unauthenticated remote attackers can directly access administrative API endpoints and perform privileged actions without a valid session.

Root Cause:
The middleware configuration restricts authentication enforcement to limited routes:

```
export const config = {
  matcher: ["/", "/dashboard/:path*"],
};
```

This leaves `/api/*` routes unprotected unless explicitly secured, which is not consistently implemented.

Impact:
An unauthenticated attacker can:

- Export the full application database
- Import or overwrite database contents
- List and generate API keys
- Retrieve provider credentials and secrets
- Modify application settings
- Trigger server-side requests (SSRF)
- Remotely shut down the server

This results in full compromise of confidentiality, integrity, and availability.

Attack Vector:
Remote, unauthenticated

Affected Components:

- `/api/settings/database`
- `/api/keys`
- `/api/providers/client`
- `/api/settings`
- `/api/provider-nodes/validate`
- `/api/shutdown`

Example Vulnerable Behavior:
Administrative API endpoints perform sensitive actions without validating authentication tokens or user permissions.

Severity:
Critical

CVSS v3.1 Vector:
AV:N / AC:L / PR:N / UI:N / S:U / C:H / I:H / A:H
Score: 9.8 (Critical)

Recommendations:

- Enforce authentication and authorization checks on all `/api/*` endpoints
- Do not rely solely on middleware-based route matching for security boundaries
- Implement centralized authentication validation for all sensitive operations
- Apply principle of least privilege
- Sanitize and restrict outbound requests to mitigate SSRF
- Remove or secure administrative endpoints such as shutdown
- Rotate all exposed secrets and API keys

Balithoth 2 weeks ago

Can you share some POC so we can have free API lol

😄 1

nabz-polo 2 weeks ago

cant deny this was ai coded

😄 1

decolua 2 weeks ago · edited by decolua Edits Owner • • •

Fixed in the latest version, thank you for reporting.

decolua closed this as completed 2 weeks ago

Metadata

Assignees

No one assigned

Labels

No labels

Projects

No projects

Milestone

No milestone

Relationships

None yet

Development

Code with agent mode

No branches or pull requests

Participants