COMMUNITY CONTENT

Submit #790003: 9Router Router 0.3.47-0.3.32 Authorization Bypass

Title	9Router Router 0.3.47-0.3.32 Authorization Bypass
Description	Missing Authentication on Administrative API Endpoints Leads to Full System Compromise in 9Router 9Router applies its login boundary to `/dashboard` routes but does not enforce equivalent server-side authentication on multiple sensitive `/api/*` handlers. As a result, an unauthenticated remote attacker can directly call administrative API routes to export the full local database, list and mint API keys, retrieve provider secrets, modify application settings, trigger server-side requests to attacker-chosen destinations, and stop the service. This is a broad administrative API exposure issue with multiple concrete impacts, all reachable without a valid session token. Exploit_Poc_Repo = https://github.com/deepcat1337/Free_Api_Exploit/tree/main
Source	⚠ https://github.com/decolua/9router/issues/431
User	cyberthoth (UID 28322)
Submission	03/26/2026 12:05 PM (14 days ago)
Moderation	04/08/2026 07:43 PM (13 days later)
Status	Accepted
VulDB entry	358280 [decolua 9router up to 0.3.47 Administrative API Endpoint /api authorization]
Points	20

Community Content

Submissions are made by VulDB community users. VulDB is *not responsible* for their content nor the links to external sources.

Please use the raw information shown and the links listed *with caution*. They might contain malicious and harmful actions, code or data.

The corresponding VulDB entries contain the moderated, verified, and normalized information provided within the raw submission.

Documentation

- Submission Policy
- Data Processing
- CVE Handling