

4

Regex account takeover

Share:



SUMMARY BY ROCKET.CHAT



Summary:

get admin reset token with authenticated user

Description:

normal user login can access to admin reset token and set a new password for admin user

Releases Affected:

- 3.18.5
- 3.0.5

Steps To Reproduce (from initial installation to vulnerability):

(Add details for how we can reproduce the issue)

1. login with low privilege user
2. copy rc_uid and rc_token for script
3. request for admin email password you can find admin mail with the script
4. run python script to get reset token with "blind no SQL injection" (regex search)

Supporting Material/References:

-

Suggested mitigation

- [list any suggested patches or steps to mitigate the problem]

Impact





the attacker can get MongoDB and search in msg database still user saved password

Fix

3.18.6, 4.4.4 and 4.7.3>

	ghaem51 submitted a report to Rocket.Chat.	May 25th (6 months ago)
	ghaem51 posted a comment.	May 25th (6 months ago)
	mrrorschach posted a comment.	May 25th (6 months ago)
	ghaem51 posted a comment.	May 25th (6 months ago)
	ghaem51 posted a comment.	May 25th (6 months ago)
	ghaem51 posted a comment.	May 25th (6 months ago)
	mrrorschach posted a comment.	May 25th (6 months ago)
	mrrorschach changed the status to Triaged .	May 25th (6 months ago)
	ghaem51 posted a comment.	May 25th (6 months ago)
	mrrorschach posted a comment.	May 26th (6 months ago)
	ghaem51 posted a comment.	Updated May 28th (6 months ago)
	ghaem51 posted a comment.	Jun 8th (6 months ago)
	mrrorschach posted a comment.	Jun 8th (6 months ago)
	mrrorschach closed the report and changed the status to Resolved .	Jun 13th (6 months ago)
	ghaem51 posted a comment.	Jun 15th (5 months ago)
	mrrorschach reopened this report.	Jun 15th (5 months ago)
	mrrorschach posted a comment.	Jun 15th (5 months ago)
	ghaem51 posted a comment.	



-  [mrrorschach](#) Rocket.Chat staff closed the report and changed the status to  **Resolved.** Jun 20th (5 months ago)
-  [mrrorschach](#) Rocket.Chat staff requested to disclose this report. Sep 22nd (2 months ago)
-  [mrrorschach](#) Rocket.Chat staff disclosed this report. Sep 22nd (2 months ago)