Foreman - Bug #26087

Brute-force attack cause looping logged user in foreman

02/19/2019 02:52 PM - Dominik Hlavac Duran

Status: Closed
Priority: Normal
Assignee: Dominik Hlavac Duran
Category: Authentication

Target version:

Difficulty: 

Pull request: https://github.com/theforeman/foreman/pull/6519

Triaged: Yes

Fixed in Releases: 1.22.0

Bugzilla link: 1654620

Found in Releases:

Description

Description of problem:
When I'm logged in UI and somebody triggers brute-force attack protection by number of failed UI logins, mine session hangs in infinite reload loop

Version-Release number of selected component (if applicable):
satellite-6.5.0-5.beta.el7sat.noarch

How reproducible:
always

Steps to Reproduce:
1. Log in to UI
2. Make sure Settings -> Authentication -> failed_login_attempts_limit is set to default 30 (or set it to some lower, non-0 number)
3. In different browser/browser profile trigger brute-force attack protection by number of failed UI logins (you need to make it in below 5 minutes which is a default timeout)
4. Note how your original UI session from step "1." looks like now

Actual results:
Original UI session is in infinite reload loop

Expected results:
Either original session remains functional (preferred) or user is notified brute-force attack protection was activated and he should investigate results and try again later

Additional info:
As this way I can disconnect any user from Satellite without having any valid Satellite or OS account, should this be considered a security issue?

Associated revisions

Revision 7995d863 - 03/26/2019 03:05 PM - Dominik Hlavac
Fixes #26087 - Bruteforce attack cause reloading users sessions (#6519)

History

#1 - 02/20/2019 08:59 AM - Lukas Zapletal
This sounds like a regular and simple DDoS attack, passenger is likely having bad time serving all those requests. I recommend deploying a proxy or Apache throttling module to prevent from that. Those excessive requests must be stopped before passenger starts processing them.

I think this should be documentation only resolution - we should document how to prevent from those attacks.

#2 - 02/20/2019 12:54 PM - Marek Hulan
If passenger only tries to login user, I don’t think it’s a big issue. I actually think it’s fine that our app has a counter of failed attempts. We already have that feature in. This is just how to deal with already logged in users (in this case QE tests) that cause the brute-force alert.

For what you suggest, I don’t know how Apache would know you’re sending incorrect credentials, perhaps based on return code from login form? Is there some module for this purpose? This is not about flooding the server with requests but about trying incorrect password for multiple times and preventing you from more tries for some time if it happens...

#3 - 02/28/2019 07:55 AM - The Foreman Bot
- Status changed from Assigned to Ready For Testing
- Pull request https://github.com/theforeman/foreman/pull/6519 added

#4 - 03/26/2019 03:05 PM - Marek Hulan
- Fixed in Releases 1.22.0 added

#5 - 03/26/2019 04:01 PM - Anonymous
- Status changed from Ready For Testing to Closed

Applied in changeset 7995d863de877ba9aa6071c6943d528ce591df07.