mgr - Feature #39999

Feature # 47765 (New): mgr/dashboard: security improvements

mgr/dashboard: Prevent brute-force/dictionary attacks against existing local user accounts

05/22/2019 01:11 PM - Lenz Grimmer

Status:	New	**% Done:**	0%
Priority:	Normal		
Assignee:			
Category:	dashboard/usermgmt		
Target version:			
Source:		**Reviewed:**	
Tags:	security	**Affected Versions:**	
Backport:		**Pull request ID:**	

Description

If passwords are used as an authentication feature (no SSO enabled), there must be protection against dictionary and brute force attacks, to make it more difficult to guess passwords.

Dictionary and brute force attacks aim to guess passwords of user and machine accounts by automated testing. To prevent this, various measures or a combination of such measures can be implemented.

- Increasing time delay (e.g. doubling the waiting time for each attempt) for re-entering a password after an unsuccessful attempt.
- Locking the user account after a specified number of failed attempts (typically 5). However, with this solution it should be remembered that this requires an unlocking process and that an attacker can use this to lock accounts and make them unusable.
- Use of CAPTCHA to prevent automated probing (often used in web applications)

In order to achieve a higher level of safety, it often makes sense to combine two or more of the above measures.

Motivation: Without appropriate protection, an attacker can attempt to determine a password by simply trying out dictionary lists or automatically generated character combinations in order to misuse the corresponding user account.

Related issues:

Related to mgr - Feature #40329: mgr/dashboard: It should be possible to set ...	**Closed**
Related to mgr - Feature #25232: mgr/dashboard: Support minimum password comp...	**Closed**
Related to mgr - Feature #25229: mgr/dashboard: Provide user enable/disable c...	**Closed**
Related to mgr - Feature #24655: mgr/dashboard: Enforce password change upon ...	**Closed**
Related to mgr - Feature #40248: mgr/dashboard: As a user, I want to change m...	**Closed**
Related to mgr - Feature #40914: mgr/dashboard: REST API: security	**Fix Under Review**

History

#1 - 05/22/2019 01:54 PM - Lenz Grimmer

- Subject changed from mgr/dashboard: Prevent brute-force/dictionary attacks against existing user accounts to mgr/dashboard: Prevent brute-force/dictionary attacks against existing local user accounts

- Description updated

#2 - 07/12/2019 03:57 PM - Lenz Grimmer

- Related to Feature #40329: mgr/dashboard: It should be possible to set an expiration date for the user password added

#3 - 07/12/2019 03:57 PM - Lenz Grimmer

- Related to Feature #25232: mgr/dashboard: Support minimum password complexity rules added

#4 - 07/12/2019 03:58 PM - Lenz Grimmer

- Related to Feature #25229: mgr/dashboard: Provide user enable/disable capability added

#5 - 07/12/2019 03:58 PM - Lenz Grimmer

- Related to Feature #24655: mgr/dashboard: Enforce password change upon first login added

#6 - 07/12/2019 04:02 PM - Lenz Grimmer

- Related to Feature #40248: mgr/dashboard: As a user, I want to change my password added

#7 - 05/06/2020 09:27 AM - Lenz Grimmer

- Related to Feature #40914: mgr/dashboard: REST API: security added

#8 - 10/06/2020 10:36 AM - Ernesto Puerta

- Tags set to security

#9 - 10/06/2020 10:40 AM - Ernesto Puerta

- Parent task set to #47765

- Tags deleted (security)

#10 - 10/06/2020 10:41 AM - Ernesto Puerta

- Tags set to security

#11 - 11/03/2020 08:47 PM - Ernesto Puerta

A reference for discussion on the effectiveness of account blockout: https://owasp.org/www-community/controls/Blocking_Brute_Force_Attacks