CZMVO Alert management system

Release: 6.0

CZMVO (Alert Management System - AMS) release R6.0 is primarily focused on security, stability and involves the following updates:

1.SECURITY

1.1. USER ACCESS TO AMS

1.1.1. API settings

1.1.1.1. AMS API interface is be limited to a number of requests per given time. Client systems exceeding this quote will receive HTTP status code (429).
The purpose of this function is to prevent misbehaving clients from flooding the AMS and also to block „denial of service attacks“.
1.1.1.2. Client should be re-verified and request a token only once in **n** minutes. This is be a parameter in „Settings“.

1.1.2. API verification via OAuth 2.0

The protocol **OAuth 2.0**. will be implemented for access to API.
A parallel access will be granted via the current access (basic authentication) and a new access (OAuth2.0). Following the launch of R6.0, both types of access will be enabled to users for a period of five months so as to facilitate a smooth transfer to the new API version.

1.1.3. Adding AMS API to enable verification via OAuth 2.0

1.1.3.1. AMS Api version

The AMS API version to be used is specified by the „amsapi-version“ as HTTP header (e.g.. „ams-api-version“ 2.0). For retrospective compatibility, omitting the header will result in direction of requests to AMS API v1.0.

1.1.3.2. Http header „User-agent“

The use of the HTTP header „User-Agent“ is mandatory. Client systems must provide details about the software version. This will **remain the same as per the current practice for communication with CZMVS**. It will also serve as a check whether the software in use is identical to the software that obtained certification and to identify if certain problems relate to a specific type of clients,too.

1.1.4. Two-step authentication for the web interface

To access the web interface, a two-step authentication will be implemented. As the second step, e-mail address or Google Authenticator may be used.
Selection of the second step will be adjustable by the administrator, eventually by the user administering users of the concerned organization. As default, e-mail address will be set with an option to add others.

Národní organizace pro ověřování pravosti léčiv, z.s., IBC Pobřežní 620/3, Karlín, 186 00 Praha 8
IČ: 05851742, www.czmvo.cz

1.2. AMS SECURITY IMPROVEMENT

The following requirements are based on the findings of IT security audit (10/2022).

1.2.1. Security improvement for adding attachments

The first level will aim at the file extension. The second level will examine the actual file content.

1.2.2. Time limit for web login

After a non-activity longer than a set time, the user will be automatically logged out. (Actually 4 hours).

1.2.3. Account lock after several unsuccessful attempts

If a user enters an incorrect password several times, the corresponding account will be locked for a defined period. (Currently 3 failed attempts = 60 minutes block.)

1.2.4. Unpredictable session id

The purpose is to prevent fixation attack. After each successful login, an unpredictable session id will be generated.

1.2.5. Cookies settings change

The attributes „Secure“ and „Http Only“ will be set to prevent certain types of attacks.

1.2.6. Login page attributes settings

The parameter autocomplete=“off“ will be set for the account login page to prevent certain types of attacks.

1.2.7. Error messages unification upon login

The aim is to unify error messages in order to block guessing of valid login accounts. Currently, the error messages differ depending on whether the entered login is valid or not, which enables identification of a valid login account and cracking the password.

Národní organizace pro ověřování pravosti léčiv, z.s., IBC Pobřežní 620/3, Karlín, 186 00 Praha 8
IČ: 05851742, www.czmvo.cz