NOOL Systém správy alertů

Release: 6.0

NOOL Systém správy alertů (Alert Management System - AMS) release R6.0 se zaměřuje zejména na bezpečnost a stabilitu a obsahuje tyto hlavní úpravy:

1.ZABEZPEČENÍ

1.1. PŘÍSTUP UŽIVATELŮ DO AMS

1.1.1. API nastavení

1.1.1.1. Rozhraní AMS API je omezeno na počet dotazů za daný čas. Tato funkce má zabránit „špatně“ se chovajícím klientům, aby nezahltili systém AMS a zároveň bránit před útoky typu „denial of service attacks“.
Klient se může znovu ověřit a získat token pouze jednou za **3** minuty.

1.1.2. API ověření pomocí OAuth 2.0

Pro přístup přes API je implementován protokol **OAuth 2.0**.

1.1.3. Doplnění AMS API pro ověření pomocí OAuth 2.0

1.1.3.1. AMS Api verze

Verze AMS API, která se má použít, je specifikována pomocí „amsapi-version“ jako hlavičky HTTP.

1.1.3.2. Http hlavička „User-agent“

Použití HTTP hlavičky „User-Agent“ je povinné.

1.1.4. Dvou-faktorové ověřování pro webové rozhraní

Pro přístup do webového rozhraní je implementováno **dvou-faktorové ověřování**. Jako druhý faktor může být využit primárně **e-mail nebo Google authenticator**.
Volba typu druhého faktoru je nastavitelná administrátorem ev. uživatelem ve správě uživatelů dané organizace.

Je umožněn **postupný přechod** uživatelů po **dobu pěti měsíců** na vyšší verzi zabezpečeného přístupu do AMS. (platí pro body 1.1.2, 1.1.3 a 1.1.4).

1.2. ZVÝŠENÍ ZABEZPEČENÍ AMS

1.2.1. Zvýšení úrovně kontroly pro vkládání příloh

V prvním stupni je kontrola na koncovku souboru. V druhém stupni pak probíhá kontrola na skutečný obsah souboru.
737313506

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

1.2.2. Časový limit pro webové přihlášení

Je implementováno automatické odhlášení uživatele po definované době nečinnosti (aktuálně 4 hodiny).

1.2.3. Uzamknutí účtu po několika neúspěšných přihlášení

Pokud uživatel při přístupu do webového rozhraní zadá opakovaně nesprávné heslo, tak dojde k uzamčení účtu na definovanou dobu. (Aktuálně 3 neúspěšné pokusy = 60 minut blokace.)

1.2.4. Nepredikovatelné session id

Cílem je znemožnit „session fixation" útok. Po každém úspěšném přihlášení uživatele je generováno pro relaci nepredikovatelné *session id*.

1.2.5. Změna nastavení cookies

Jsou nastaveny atributy „Secure" a „Http Only" k zabránění některých typů útoků.

1.2.6. Nastavení atributu pro přihlašovací stránku

Je nastaven parametr autocomplete="off" pro přihlašovací stránku k zabránění některých typů útoků.

1.2.7. Nastavení unifikace chybových hlášení při přihlašování

Cílem je unifikací chybových hlášení při pokusech o přihlášení znemožnit hádání platných přihlašovacích jmen.

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