Příloha č. 1
Počet stran: 3

Specifikace služby

Bezpečnostní update Interního komunikačního portálu (dále jen „IKP“)

a) Aktualizace (update) jádra a veškerých modulů minimálně ve verzích dostupných k datu plnění. Dále uvedené aktualizace jsou minimální hodnoty a druhy známé objednateli k datu zadání zadávacího řízení.

- **Chaos tool suite (ctools) 7.x-1.12**
  Doporučená verze: 7.x-1.14 (2018-Úno-24)
  Zahrnuje: Chaos tools
- **Course 7.x-1.10**
  Doporučená verze: 7.x-1.12 (2017-Lis-22)
  Zahrnuje: Course, Course certificate, Course content, Course object manual, Course quiz
- **Devel 7.x-1.5**
  Doporučená verze: 7.x-1.6 (2018-Dub-18)
  Zahrnuje: Devel
- **Entity API 7.x-l.8**
  Bezpečnostní aktualizace: 7.x-1.9 (2018-Úno-14)
  Zahrnuje: Entity API, Entity tokens
- **Feeds Tamper 7.x-1.1**
  Doporučená verze: 7.x-1.2 (2017-Pro-lO)
  Zahrnuje: Feeds Tamper, Feeds Tamper Admin Ul
- **Global Redirect 7.x-1.5**
  Doporučená verze: 7.x-1.6 (2018-Úno-15)
  Zahrnuje: Global Redirect
- **Job Scheduler 7.x-2.0-alpha3**
  Doporučená verze: 7.x-2.0 (2018-Úno-13)
  Zahrnuje: Job Scheduler
- **Password Policy 7.x-1.14**
  Doporučená verze: 7.x-1.15 (2018-Bře-06)
  Zahrnuje: Password policy
- **Profile 2 7.x-I.3**
  Doporučená verze: 7.x-1.4 (2018-Bře-17)
  Zahrnuje: Profile2
- **Quiz 7.x-5.1**
  Doporučená verze: 7.x-5.2 (2017-Lis-15)
  Zahrnuje: Quiz, .Quiz - Directions, Quiz - Long answer, Quiz - Matching question, QUlZ - Multichoice,
  Quiz - Pages, Quiz - Scale, Quiz - Short answer, Quiz - True false, Quiz question
- **Reroute Email7.x-1.2**
  Doporučená verze: 7.x-1.3 (2017-Pro-15)
  Zahrnuje: Reroute emails
- **Views 7.x-3.18**
  Doporučená verze: 7.x-3.20 (2018-Dub-14)

Zahrnuje: Views, Views Ul

- **Views Bulk Operations (VBO) 7.x-3.4**
  Doporučená verze: 7.x-3.5 (2018-Kvě-09)
  Zahrnuje: Actions permissions (VBO), Views Bulk Operations

b) Funkční aktualizace provozních částí webové aplikace IKP provedené na základě výsledků bezpečnostních testů IKP a v souladu s navrhovanými opatřeními CIRC AKIS.

Výsledky testů:

Acunetix

HIGH: 0, MEDIUM: 12, LOW: 16, INFO: 467

Medium (7.5) lx - PHPinfo page

Medium (5.3) lx - PHP allow_url_fopen enabled

Medium (4.3) 2x - HTML form without CSRF protection (formuláře /user; /user/password; příp. další na webu)

Medium (3.1) 2x - Development configuration file

Low (7.5) 6x - Possible sensitive directories

Low (7.5) 4x - Session token in URL

Low (0.0) lx - TRACE method is enabled

FP: Medium 4x - HTML form without CSRF protection

FP: Low 4x - Login page password guessing attack

FP: Low 1 x - Insecure transition from HTTPS to HTTP in form post

Navrhovaná opatření:

PHPinfo page:

Soubor /.php je volně přístupný z Internetu a rozkrývá citlivé informace (PHP konfigurace) o nastavení a fungování webové aplikace. Lze zde vyčíst i konfigurace, které by mohly být zneužitelné známými útoky. Doporučením je tedy zakázat přístup k tomuto souboru a k dalším složkám a souborům na serveru. Při pokusu o jejich navštívení z "venku" navracet nejlépe index stránky webu.

PHP allow url fopen enabled:

V souboru /pi.php byla nalezena konfigurace, která by mohla ohrozit web. Allow_url_fopen možňuje načíst data ze vzdálených lokací, tzn., dá se zneužít v některých případech i na "code injection" útoky. Doporučením jsou úpravy v souborech php.ini: allow_url_fopen = 'off a v souboru.htaccess: php_flag allow_url_fopen off.

Development configuration file:

Soubor, který by neměl být přístupný z Internetu - /sites/all/themes/ikp7/gulpfile.js a soubor /sites/all/themes/ikp7/package.json. Rozkrývají informace o aplikaci. Doporučením je při dotazu na neexistující, či nepřístupný soubor a složku navracet žadateli index stránky webu, aby nedocházelo k poskytování indicií k napadení webu.

HTMLform without CSRF protection:

Sken nalezl formuláře, které by mohly být ovlivnitelné přes Cross Site Request Forgery, pokud neobsahují obrany proti této mechanice. Jelikož webová aplikace obsahuje funkce, které by mohly být zneužity, a to zejména po přihlášení, doporučuje se ošetřit session a formuláře proti CSRF zneužití. Hlavní technikou proti CSRF je anti-CSRF token (ticket per session), který se přidá na všechny odkazy a formuláře,

které mají v aplikaci důležitější význam (tzn., že searchfield není třeba ošetřit, ale např. změna hesla a funkcionality po přihlášení ANO). Jednotlivé body, co by měl token splňovat, jsou uvedeny i v developer reportu pod danou zranitelností.

Possible sensitive directories:

Na serveru se nacházejí složky, které nejsou přímo pro linkovány z webu, ale jdou odhalit skenovacím nástrojem, jelikož při dotazu na ně se zobrazí odpověď serveru o zamítnutém přístupu. Nejsou tedy přístupné a v tomto případě ani názvy složek nerozkryjí důležité informace o webu.

Správný postup, jak skrýt obsah bez vyzrazení indicií o aplikaci je takový, že každá odpověď serveru na skryté i na neexistující složky/soubory bude stejná, nejlépe pouhá na vrácení indexu stránky.

Session token in URL:

Sken nalezl při načtení obrázku CAPTCHA v URL také záznam o session ID. Tento údaj se nedoporučuje přenášet v URL kvůli možnému ukradení referrer záznamu, se kterým by se session ID také přeneslo. V tomto případě, pokud se session ID vyskytuje v URL pouze při načítání CAPTCHA, není prostor pro ukradení hlavičky referrer třetí stranou. Není to tedy v tomto případě bezpečnostní problém.

TRACE method is enabled:

Sken detekoval povolenou metodu TRACE. Díky ní se ze serveru ke klientovi můžou navracet informace zasílané v hlavičkách komunikace původně jen směrem k serveru. To by mohlo být zneužíváno v případě client-side útoků k ukradení citlivých údajů - např. přihlášení k účtu na webu.

Doporučením je zakázat metodu TRACE a příp. i jiné metody, které není nutné aktuálně využívat.

c) Zabezpečení aplikace obecného nařízení Evropského parlamentu a Rady o ochraně osobních údajů č. 2016/679 (GDPR) a dalších navazujících právních předpisů České republiky a vnitřních předpisů Ministerstva obrany, k zabezpečení ochrany osobních údajů ve webové aplikaci IKP na minimální úrovni splňující uvedené normy.

d) Po provedení bezpečnostního update IKP, funkční aktualizace provozních částí a aplikace obecného nařízení Evropského parlamentu a Rady o ochraně osobních údajů č. 2016/679 (GDPR) včetně souvisejících předpisů, otestovat funkčnost a bezchybnost všech částí IKP (včetně databázových a redakčních). Testování realizovat jak poskytovatelem, tak testem CIRC AKIS spoluprací vyžádanou poskytovatelem. Testování redakční části realizovat cestou redakce IKP (oddělení plánování lidských zdrojů odboru řízení lidských zdrojů Sekce státního tajemníka Ministerstva obrany). Správnost instalace aktualizací a navazujících úprav provozních částí potvrdit akceptačním řízením, jehož nedílnou součásti jsou protokoly potvrzující aktualizovaný a funkční stav ke dni akceptace.