Kopsavilkums

Testa rezultātos ir konstatēti augsta un vidēja līmeņa riski, kas attiecas uz sistēmas ievainojamību, pārsvarā vienā no funkcionalitātēm –

Lietotāju un mašīnu

# 3. Pārbaužu rezultāti

## 3.1. Risku klasifikācija

Turpmāk nodaļā ir izmantota šāda risku klasifikācija:

3 – riski, kas ievērojami ietekmē aplikāciju un datu drošību - to mazināšanai būtu jāpievērš pastiprināta un tūlītēja uzmanība;

2 – riski, kas ietekmē aplikāciju drošību, kā rezultātā to mazināšana būtu jāplāno vidējā termiņā (1-3 mēneši);

1 – mazāk būtiski riski, vai neatbilstības pret labāko praksi, kam nav tiešas ietekmes uz IT sistēmu un informācijas drošību – šādu risku mazināšanas aktivitāšu realizācija būtu jāveic atkarībā no pieejamajiem resursiem.

| | | | | |
|---|---|---|---|---|
| 2. | Testēšanas gaitā, kā konkrēta uzņēmuma lietotājam (administratoram), konstatēta iespēja dzēst citu uzņēmumu piegādes adreses. Vizuāli šāda iespēja netiek atainota. | Neautorizēta piekļuve neparedzētai funkcionalitātei - iecerētās biznesa loģikas apiešana, tiešs datu integritātes apdraudējums. | 3 | Rekomendējam veikt izmaiņas tīmekļa aplikācijas pirmkodā, nodrošinot validāciju HTTP POST pieprasījuma laukos atbilstoši iecerētajai biznesa loģikai. |

3.Kategorijas, jeb kritiskas ievainojamibas atrastas vienā sistēmas funkcionalitātes blokā, tādēl uz 05.06 (sanāksmes brīdi) novērstas . Retesti parādīs rezultātu. Ticams, ka 07.06 rezultāts būs zināms.

| | | | | |
|---|---|---|---|---|
| 16. | Pārbaužu laikā konstatēta iespēja uzsākt TL pārrakstīšanu (nodošanu lietošanā) transporta līdzekļiem, kas pieder citiem (ar konkrēto lietotāju nesaistītiem) uzņēmumiem. | Neautorizēta piekļuve citu uzņēmumu resursiem/datiem; datu integritātes apdraudējums. | 2 | Rekomendējam veikt validāciju minētajā funkcionalitātē, nodrošinot iespējas uzsākt TL pārrakstīšanu tikai TL-iem, kas saistīti ar konkrētā lietotāja uzņēmumu. |

2.Kategorijas, Jeb riski kuru novēršana jāplāno 1-3 mēnešu terminā, tiks novērsti nepilnas nedēļas laikā, jo arī šeit, pārsvarā tie ir vienveidīgi, un līdz Jūnija 3 dekādei būs pārtestēti.

| | | | | |
|---|---|---|---|---|
| 33. | Testēšanas gaitā konstatēti izsmeļoši kļūdas paziņojumi SOAP API XML augšupielādes funkcionalitātē, piemēram:<br><faultstring>500: unable to retreive classifier (/api/openapi/token/organization_by_global/1.2.3.4.5): Client error: `GET https://admina.kpdc.lv/api/openapi/token/organization_by_global/1.2.3.4.5` resulted in a `400 Bad Request` response:<br>{"error":"Bad request"}<br>Path: MeasuringTicket/MeasuringTicketHeader/OtherParty/0</faultstring> | Pastāv risks, ka šāda informācija tiks izmantota uzbrukuma gadījumā, lai konkretizētu risinājumu versijas, konfigurāciju, izvietojumu tādējādi paaugstinot neautorizētas piekļuves iespēju. | 1 | Rekomendējam veikt izmaiņas risinājuma konfigurācijā, liedzot detalizētu kļūdu paziņojumu attēlošanu. |

1.Kategorijas, Jeb riski vai nepilnības kas tieši neietekmē sistēmas drošību, kur normāla prakste ir izvērtēt un lemt par to realizēšanu vai nē.
Piemēram augstāk redzamais – nerealizēsim.

| PĀRBAUDE | KONSTATĒJUMI |
| --- | --- |
| Neautentificētas piekļuves testi aplikācijas iekšējām sadaļām. | Tika izmēģināti vairāki varianti iecerētā autentifikācijas mehānisma apiešanai ar mērķi iegūt piekļuvi autentificētu lietotāju un administrācijas sadaļām, t. sk.:<br>• manuāli pārlasot un pieprasot aplikācijas ceļus/direktorijas;<br>• SQL injekcijas;<br>• Parametru maiņa;<br>• Sesijas id paredzēšana.<br><br>Taču pilnvērtīgas iespējas piekļūt aplikācijas funkcionalitātēm, kas paredzētas autentificētiem lietotājiem, ar |
| Aplikācijas lietotāju reģistrācijas procesa nepilnības. | Izmantojamas ievainojamības netika identificētas. |
| Pieprasījuma Injekciju testi, t. sk. SQL, LDAP, ORM, SSI, XML un tml. | • SQL injekciju iespējas netika konstatētas aplikācijas sadaļās.<br>• LDAP injekcijas netika konstatētas;<br>• SSI izpilde netika konstatēta;<br>• XML injekciju iespējas netika konstatētas;<br>• Citas injekciju iespējas netika konstatētas. |

Fiksēti visi veiktie testi, kā rezultātā dokumentā ir 30 l.p.p. ar pārbaudēm un konstatējumiem, kas ļauj saprast visu kas ir testēts.