מבדק חדירות

אתר מילואים אישי

צוות אבטחת מידע

דצמבר, 2015

מסמך זה מכיל מידע רגיש אודות תשתיות ממשל זמין ורמת אבטחת המידע בהן.
אין להעביר מסמך זה ללא אישור מנהל אבטחת המידע של ממשל זמין

תוכן עניינים

1. מאפייני מסמך 3
2. כללי 4
   2.1. הקדמה 4
   2.2. תיאור המערכת 4
   2.3. סיכום ממצאים טכניים 4
   2.4. הנחת יסוד 4
3. סיכום התוצאות 5
4. ממצאים 6
   4.1. שינוי פרטי משתמש אינו דורש הזנת סיסמא בשנית 7
   4.2. *המערכת שומרת ומציגה מידע רגיש בעת שינוי סיסמא* 8
   4.3. העלאת קובץ זדוני לשרת 9
   4.4. *המערכת מאפשרת גישה ממקור חיצוני באמצעות פלאש* 12
   4.5. *שימוש לקוי במנגנון CAPTCHA* 13

מסמך זה מכיל מידע רגיש אודות תשתיות ממשל זמין ורמת אבטחת המידע בהן.
אין להעביר מסמך זה ללא אישור מנהל אבטחת המידע של ממשל זמין

1. מאפייני מסמך

מחבר	אודי ברוך
מבקר	
מספר גרסה	1.0
סטטוס	
תאריך הוצאה	
שם קובץ אלקטרוני	

תשומות / הערות

שם/תפקיד	הערה (אופציונאלי)	תאריך	חתימה

היסטוריה

מ. גרסה	ת. הוצאה	מחבר	שינויים מרכזיים בגרסה
1.0	28.12.2015	אודי ברוך	דוח ראשון

הפצה

מ. גרסה	נמענים

מסמך זה מכיל מידע רגיש אודות תשתיות ממשל זמין ורמת אבטחת המידע בהן.
אין להעביר מסמך זה ללא אישור מנהל אבטחת המידע של ממשל זמין

2. כללי

2.1 הקדמה

מסמך זה מתאר את ממצאי בדיקת החדירות שבוצעה על אתר מילואים אישי במהלך חודש דצמבר 2015, שארכו כשבוע ימים.

הבדיקה בוצעה על ידי צוות אבטחת מידע של ממשל זמין, באמצעות בודקי חדירות מוסמכים, המיומנים בתקיפת יישומים ותשתיות.

2.2 תיאור המערכת

המערכת מרכזת מידע לאנשי המילואים.
במערכת ניתן לצפות ולאשר צווי מילואים ולבצע שינוי פרטים אישיים והגשת בקשות.

2.3 סיכום ממצאים טכניים

במערכת, זוהו חולשות אבטחת מידע, המאפשרות לתוקף כלשהו מרשת האינטרנט, לממש חלק מתרחישי האיום, ובכלל זאת:

1. גורם כלשהו תוקף את משתמשי המערכת.
2. גורם כלשהו מצליח לחשוף מידע חיוני על המערכת.
3. גורם כלשהו עשוי לנצל פרצות אבטחה באתר עקב יישום ופיתוח לא מאובטח.

חשיפת המערכת לרשת האינטרנט במצבה הנוכחי ,מהווה סיכון לפגיעה בתהליכים העסקיים של המערכת, במשתמשי המערכת ובמערכות המחשוב המקושרות אליה.

2.4 הנחת יסוד

1. הסביבה שנבדקה הינה סביבה חיצונית למטרת בדיקות בלבד, יש לציין שהסביבה אינה יציבה והדבר מנע סריקות אוטומטיות ולכן נבדקה בצורה ידנית בלבד. יש לדאוג לסביבת בדיקות יציבה ולבצע בדיקה חוזרת בעתיד (בנוסף זמן הבדיקה בפועל שונה ממסגרת זמן הבדיקה שהוקצה כתוצאה מכך).
2. המערכת נמצאת בסביבת טסט ולכן לא צוינו ממצאי תשתית. במעבר לסביבת הייצור בתווך מוצפן יש לשים לב כי מוגדר מאפיין ה- Secure ב- Cookie.
3. דוח זה הופק לפני ביצוע סקר קוד לאתר ולכן ייתכן והדוח יתעדכן בהמשך.

מסמך זה מכיל מידע רגיש אודות תשתיות ממשל זמין ורמת אבטחת המידע בהן.
אין להעביר מסמך זה ללא אישור מנהל אבטחת המידע של ממשל זמין

3. סיכום התוצאות

במהלך המבדק, סווגו הממצאים השונים על פי 4 רמות חומרה אשר נקבעו מראש. רמת חומרת הממצאים נקבעה על בסיס הסיכון הנשקף לארגון בעקבות מימוש החשיפה. להלן רמות החומרה:

קריטית – קיים איום מיידי לתהליכים עסקיים בארגון.

גבוהה – קיים איום ישיר לתהליכים עסקיים בארגון.

בינונית – קיים איום עקיף/חלקי לתהליכים עסקיים בארגון.

נמוכה – לא קיים איום ישיר, אך ניתן לנצל את הפגיעות כדי לבצע תקיפות נוספות.

מסמך זה מכיל מידע רגיש אודות תשתיות ממשל זמין ורמת אבטחת המידע בהן.
אין להעביר מסמך זה ללא אישור מנהל אבטחת המידע של ממשל זמין

4. ממצאים

להלן ריכוז כלל הממצאים, שזוהו במסגרת בדיקת החדירות:

מס'	תיאור הממצא	רמת חומרה
4.1	שינוי פרטי משתמש לצורך איפוס סיסמא אינו דורש הזנת סיסמא בשנית	**גבוהה**
4.2	המערכת שומרת ומציגה מידע רגיש בעת שינוי סיסמא	**גבוהה**
4.3	העלאת קובץ זדוני	**גבוהה**
4.4	המערכת מאפשרת גישה ממקור חיצוני באמצעות פלאש	**בינונית**
4.5	שימוש לקוי במנגנון CAPTCHA	**בינונית**

מסמך זה מכיל מידע רגיש אודות תשתיות ממשל זמין ורמת אבטחת המידע בהן.
אין להעביר מסמך זה ללא אישור מנהל אבטחת המידע של ממשל זמין

4.1 שינוי פרטי משתמש אינו דורש הזנת סיסמא בשנית

רמת חומרה: ***גבוהה***

סיווג ממצא: *Input and Data Validation*

תיאור הבעיה

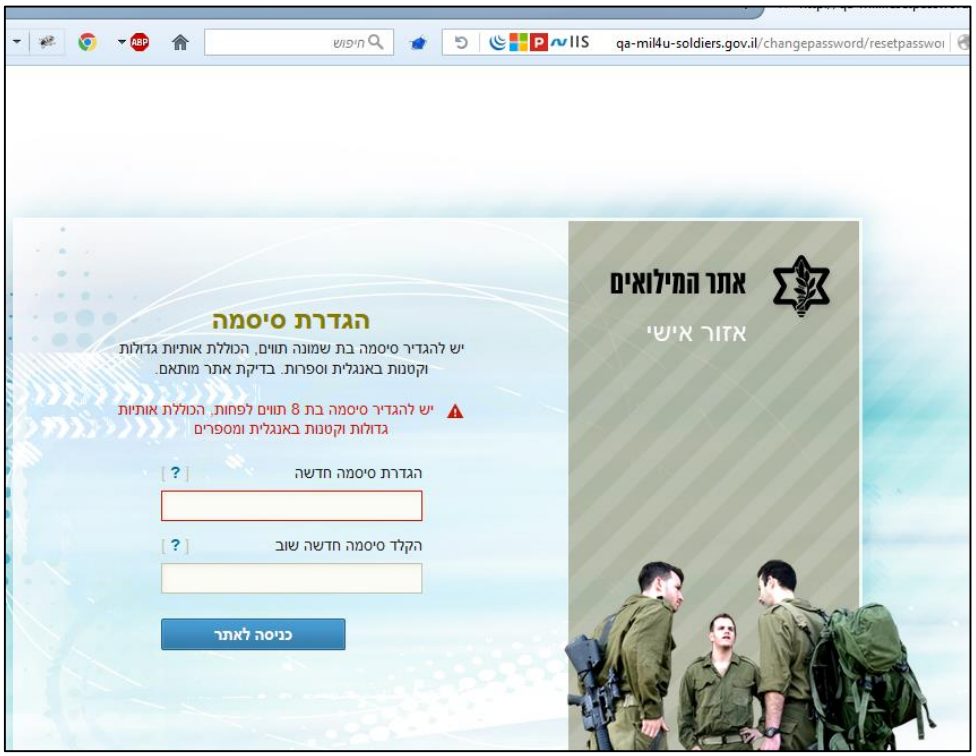
המערכת אינה מאלצת את המשתמשים להזין את סיסמתם בשנית לצורך החלפה לסיסמא חדשה.
כך תוקף יכול לשנות את סיסמת הגולשים ללא ידיעת הסיסמא הקיימת.

פרטים טכניים

המערכת אינה מאלצת את המשתמשים להזין את סיסמתם בשנית לצורך ביצוע שינויים בפרטיהם האישיים.
על-ידי גישה לקישור מסויים במערכת באופן ישיר, המערכת אינה מאלצת את המשתמש להזין את סיסמתו בשנית לצורך קביעה של סיסמא חדשה.

הוכחת קיום ממצא:

הנתיב:
http://qa-mil4u-soldiers.gov.il/changepassword/resetpassword



המלצות לתיקון

במערכת יש מנגנון המחייב הכנסת סיסמא קיימת לפני שינוי הסיסמא לאחת חדשה ולכן יש להסיר נתיב זה.

מסמך זה מכיל מידע רגיש אודות תשתיות ממשל זמין ורמת אבטחת המידע בהן.
אין להעביר מסמך זה ללא אישור מנהל אבטחת המידע של ממשל זמין

4.2 ***המערכת שומרת ומציגה מידע רגיש בעת שינוי סיסמא***

רמת חומרה: ***גבוהה***

סיווג ממצא: *Input and Data Validation*

תיאור הבעיה

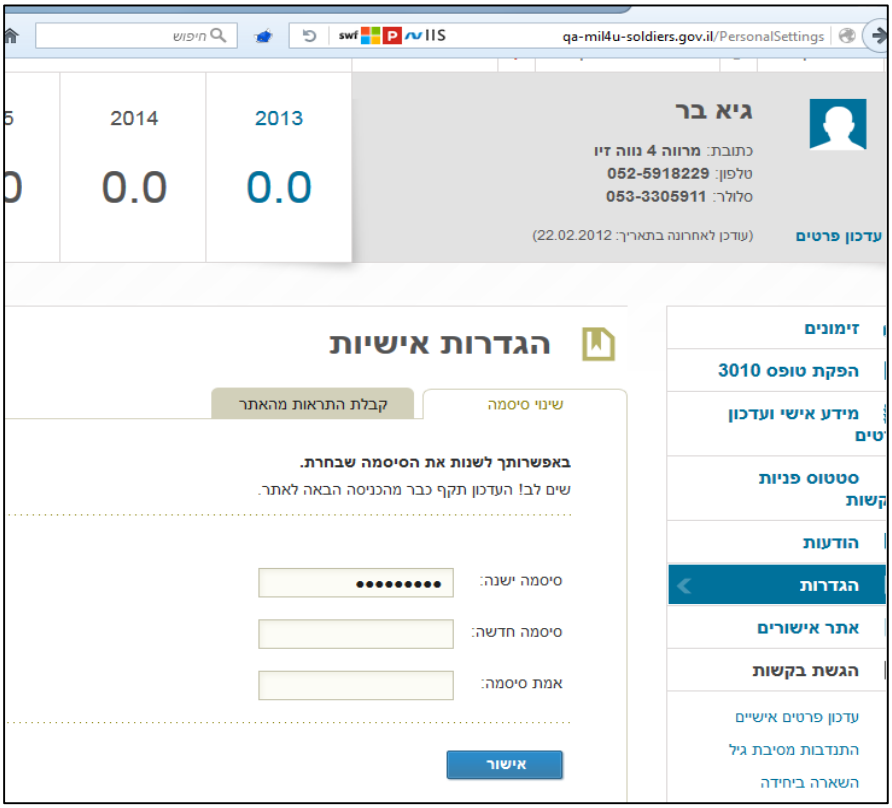
בהחלפה סיסמא חדשה, המערכת מבקשת להזין את הסיסמא הקיימת, המערכת שומרת את סיסמת המשתמש מנתוני ההתחברות (cache) ומזינה את השדה באופן אוטומטי ובכך פוגעת המנגנון כולו.
כך תוקף יכול לשנות את סיסמת הגולשים ללא ידיעת הסיסמא הקיימת.

פרטים טכניים

המערכת שומרת את סיסמת המשתמש מנתוני ההתחברות ומזינה את השדה באופן אוטומטי ובכך פוגעת המנגנון כולו.

הוכחת קיום ממצא:

הנתיב:
http://qa-mil4u-soldiers.gov.il/PersonalSettings



המלצות לתיקון

אין לאפשר לדפדפן למלא שדה זה באופן אוטומטי, יש להפריד את זיהוי השדה הנ"ל מזיהוי השדה של עמוד ה- Login.

מסמך זה מכיל מידע רגיש אודות תשתיות ממשל זמין ורמת אבטחת המידע בהן.
אין להעביר מסמך זה ללא אישור מנהל אבטחת המידע של ממשל זמין

4.3 העלאת קובץ זדוני לשרת

רמת חומרה: ***גבוהה***

סיווג ממצא: D.O.S

תיאור הבעיה

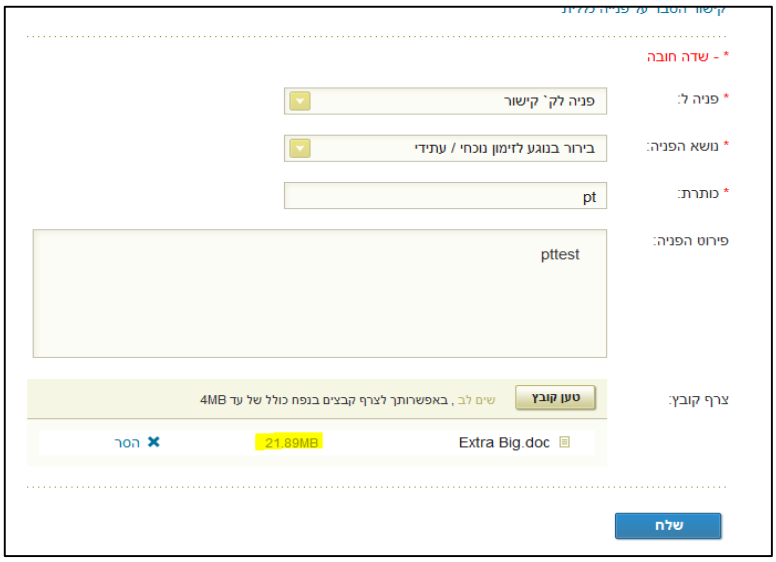
בדפי המערכת קיימת אפשרות העלאת קבצים. כאשר קובץ מועלה לשרת, מתבצעות בדיקות סוג ותקינות של הקובץ. למרות זאת, השרת מאפשר העלאה של קבצי Word גדולים מהמגבלה הקיימת וקבצי EXE אסורים.

פרטים טכניים

השרת מאפשר העלאה של קבצים אסורים לפי המגבלות של האתר, המערכת מבצעת בדיקה **רק בצד לקוח** ולא בצד שרת.
על ידי כך ניתן לפגוע בשרת במספר צורות, אם בקוד זדוני ואם בניצול מקום בזכרון עד אפס מקום על ידי העלת קבצים גדולים.

הוכחת קיום ממצא:

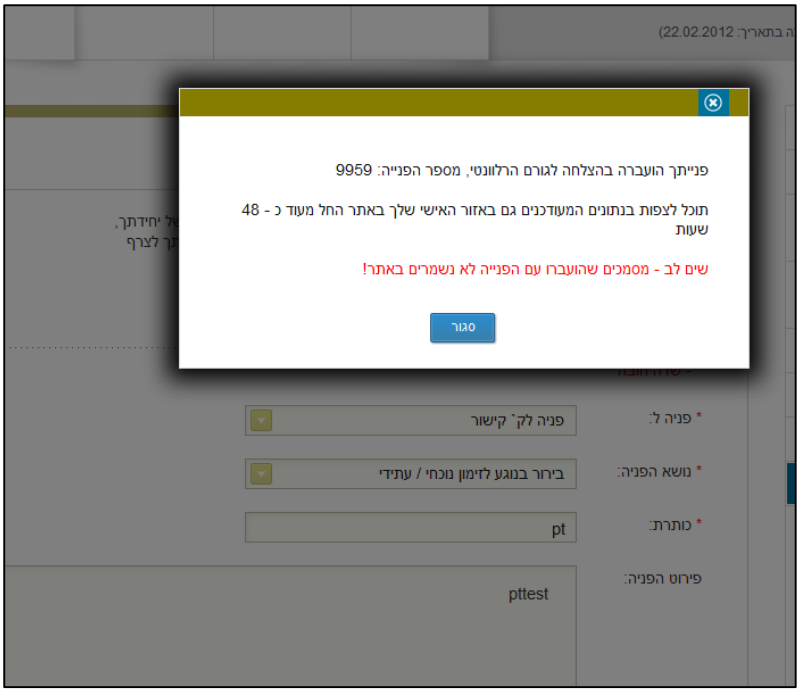
העלאת קובץ בגודל של מעל מ 20MB



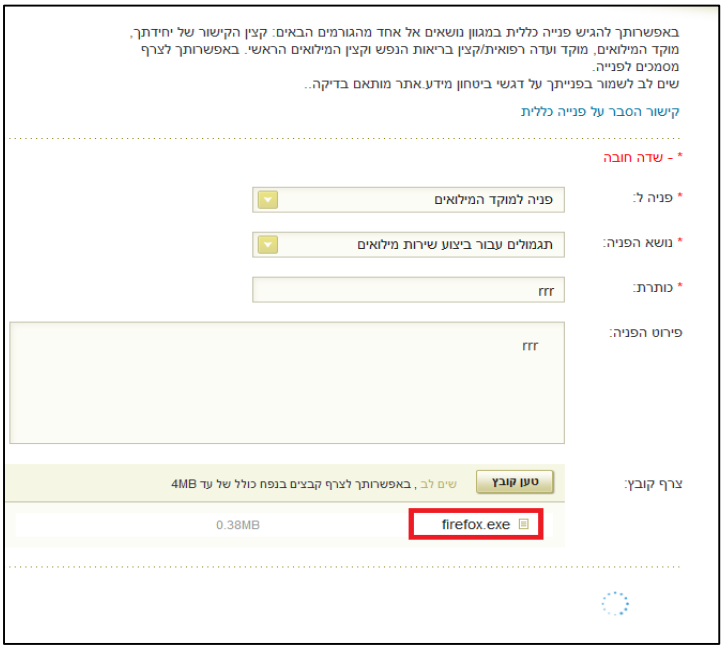

```
}

var IdComplete = 0;
var MarriageCertComplete = 0;
var PAppendixComplete = 0;
var ChAppendixComplete = 0;
var PermitComplete = 0;
var DraftComplete = 0;
var AAppendixComplete = 0;
var TimetableComplete = 0;
var BoardComplete = 0;
var GeneralFilesComplete = 0;
var removeStr = 'עבוקה תא ריסהל דנוצרבש חוטב תחא מאה ';
var maxFilesSize = 26096000;
var fileSizeStr = 'דבלב 20MB דע לש ללוכ חפנב סיצבק חרצל ןתינ';
var nofilesStr = 'מ-4 MB לודג וא המישרב סייק רבכ חיסוהל דנוצרבש עבוקה';
var enableFileExtensions = ',doc,docx,jpg,jpeg,png,pdf,tif,tiff,';
var fileExtensionStr = 'נוסח סיצבק קר תולעהל ןתינ: \n doc, docx, jpg, jpeg, \n png, pdf, tif, tiff';
var validFileExp = /^[0-9a-zA-Z _,. ]+$/;
```

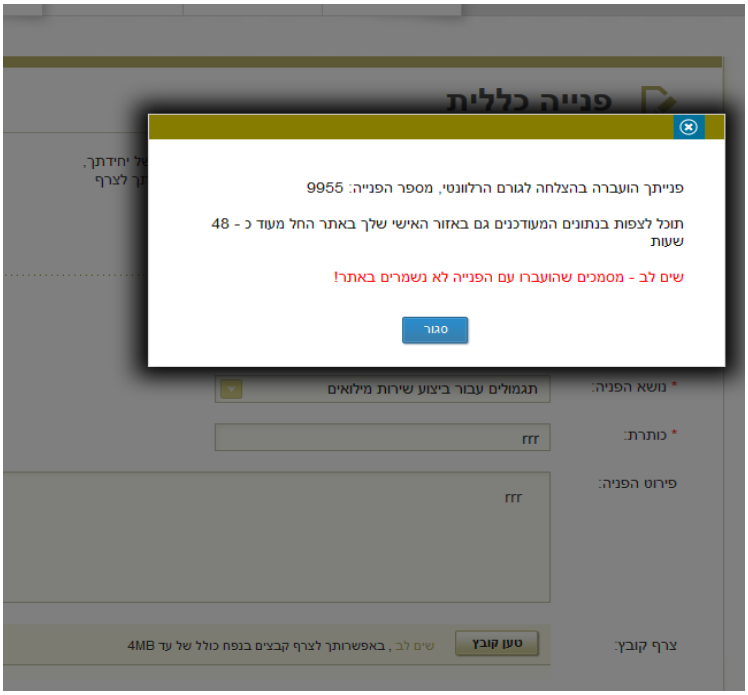
מסמך זה מכיל מידע רגיש אודות תשתיות ממשל זמין ורמת אבטחת המידע בהן.
אין להעביר מסמך זה ללא אישור מנהל אבטחת המידע של ממשל זמין



העלאת קבצים זדוניים בסיומת EXE



מסמך זה מכיל מידע רגיש אודות תשתיות ממשל זמין ורמת אבטחת המידע בהן.
אין להעביר מסמך זה ללא אישור מנהל אבטחת המידע של ממשל זמין



<u>המלצות לתיקון</u>

- יש לבצע בדיקה של גודל תוכן המועבר בבקשה הנשלחת לשרת.
- יש לבדוק את סוג הקבצים בצד השרת ולא לאפשר העלאה של קבצים אסורים.

מסמך זה מכיל מידע רגיש אודות תשתיות ממשל זמין ורמת אבטחת המידע בהן.
אין להעביר מסמך זה ללא אישור מנהל אבטחת המידע של ממשל זמין

4.4 המערכת מאפשרת גישה ממקור חיצוני באמצעות פלאש

רמת חומרה: ***בינונית***

סיווג ממצא: *Configuration*

תיאור הבעיה

אתרי צד שלישי זדוניים יכולים לגרום למשתמשי קצה לבצע פעולות במערכת ללא ידיעתם. התקפה זו עלולה לאפשר לתוקפים מרשת האינטרנט לתקוף את משתמשי המערכת, לאסוף מידע פרטי על משתמשי האתר ועוד.

פרטים טכניים

שרת האפליקציה מאפשר גישה בפלאש מכל דומיין, הקובץ Crossdomain.xml מגדיר האם אפליקציית פלאש יכולה לגשת למשאב במערכת מדומיין אחר.
כאשר ההרשאות לא מוגבלות ניתן לנצל זאת להתקפות כמו: CSRF ו- XSS.

הוכחת קיום ממצא:

המלצות לתיקון

יש להגדיר את המאפיין allow-access-from מקובץ Crossdomain.xml כך שיכיל דומיין ספציפי בלבד ולא כל דומיין.

מסמך זה מכיל מידע רגיש אודות תשתיות ממשל זמין ורמת אבטחת המידע בהן.
אין להעביר מסמך זה ללא אישור מנהל אבטחת המידע של ממשל זמין

4.5 ***שימוש לקוי במנגנון CAPTCHA***

רמת חומרה: ***בינונית***

סיווג ממצא: Implementation

תיאור הבעיה

השימוש ב- CAPTCHA במסך ההתחברות נמצא לקוי ואינו חוסם בפועל ניסיונות.
המנגנון אינו בודק את פתרון ה- Captcha שאכן הערך המוזן על ידי המשתמש הוא נכון בעת הכנסת סיסמא תקינה (לאחר מספר ניסיונות כושלים).

פרטים טכניים

השימוש ב- CAPTCHA במסך ההתחברות נמצא לקוי.
לאחר מספר נסיונות מופיעה CAPTCHA אך בהכנסת סיסמא תקינה המערכת מאפשרת התחברות גם ללא הכנסת ה-CAPTCHA.

המלצות לתיקון

- יש להטמיע הגנות CAPTCHA בכל הטפסים המאפשרים למשתמש לשלוח פניות מצטברות או להעלות תוכן (בצורה רוחבית באתר).
- יש לוודא כי המשתמש מזין ערך גם בהזנת סיסמא תקינה.

מסמך זה מכיל מידע רגיש אודות תשתיות ממשל זמין ורמת אבטחת המידע בהן.
אין להעביר מסמך זה ללא אישור מנהל אבטחת המידע של ממשל זמין