מבדק חדירות

אתר אחים לנשק
של מנהל האוכלוסיות

צוות אבטחת מידע

יולי, 2015

תוכן עניינים

1. מאפייני מסמך 3
2. כללי 4
   2.1. הקדמה 4
   2.2. תיאור המערכת 4
   2.3. סיכום ממצאים טכניים 4
3. סיכום התוצאות 5
4. ממצאים 6
   4.1. *אין שימוש ב- CAPTCHA* 7
   4.2. לא קיימת הגנה מפני התקפת Clickjacking 9
   4.3. שירותים לא מוקשחים חושפים מידע פנימי אודות המערכת 11

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	08.07.2015	אודי ברוך	דוח ראשון

הפצה

מ. גרסה	נמענים

2. כללי

2.1 הקדמה

מסמך זה מתאר את ממצאי בדיקת החדירות שבוצעה על מערכת אחים לנשק במהלך חודש יולי 2015, שארכו כיומיים.

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

2.2 תיאור המערכת

מנהל אוכלוסיות הינה מחלקה המשתייכת פיקודית לאגף כוח אדם, ותפקידה לטפל בכל האוכלוסייה הלא יהודית המשרתת בצה"ל.
מנהל אוכלוסיות פועל במספר תחומים בנושא גיוס, השכלה ותעסוקה, ייצוג והסברה, פרט ונפגעים ופרויקטים ייחודיים.

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 משאבי המערכת.
2. גורם כלשהו מצליח לחשוף מידע חיוני על המערכת.

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.

4. ממצאים

להלן ריכוז כלל הממצאים, שזוהו במסגרת בדיקת החדירות:

מס'	תיאור הממצא	רמת חומרה
Error! Reference source not found.Error! Reference source not 1found.	אין שימוש ב- CAPTCHA	**גבוהה**
Error! Reference source not 2found.	Clickjacking	נמוכה
Error! Reference source not found.Error! Reference source not 3found.	שירותים לא מוק שחים חושפים מידע פנימי אודות המערכת	נמוכה

4.1 ***אין שימוש ב- CAPTCHA***

רמת חומרה: ***גבוהה***

סיווג ממצא: *Denial of Service*

תיאור הבעיה

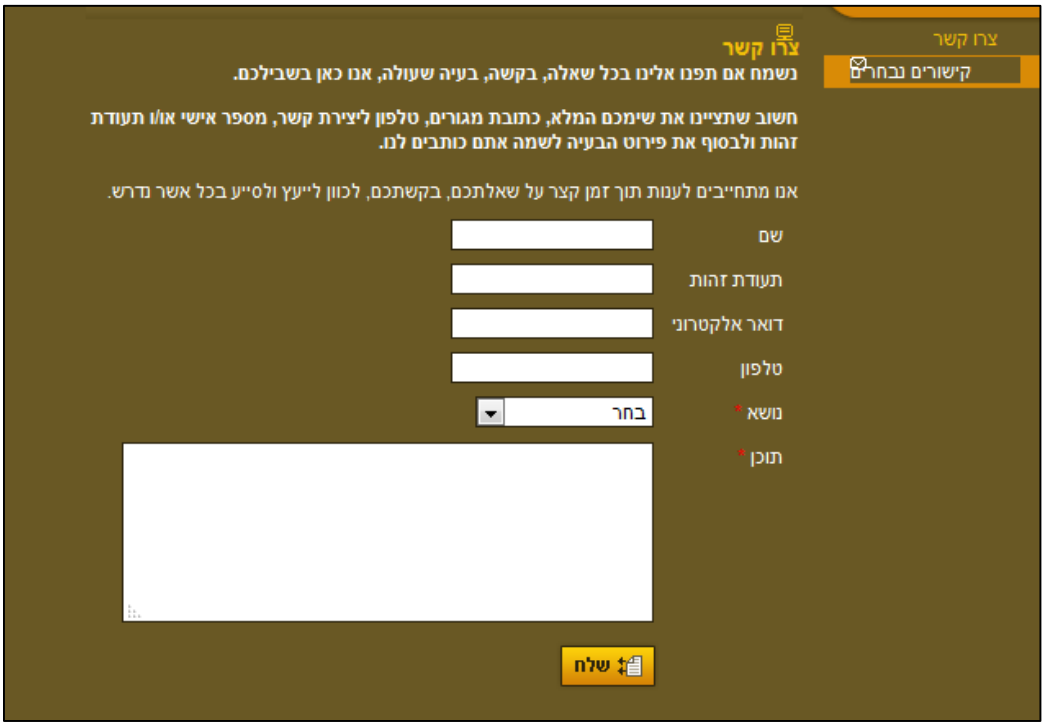
פורצים מסוגלים לבצע נסיונות חוזרים של שליחת דואר מרובות וללא הגבלה, וזאת בעקבות אי קיומם של מנגנוני הגנה מפניות ממוחשבות אוטומטיות. להעדרם של מנגנוני הגנה אלו יש השלכות נוספות; פורץ עשוי לנסות להציף את המערכת בפניות על מנת לנצל את משאבי המערכת, ובצורה זו למנוע מהמערכת לקבל פניות חדשות או לתפקד כראוי.

פרטים טכניים

המערכת מאפשרת למשתמשים לשלוח פניות שונות דרך ממשק המשתמש. ממשקי המערכת אינם מוודאים כי הפניות שהתקבלו מצד המשתמש נשלחו על ידי משתמש אנושי (ולא באופן אוטומטי) ובעקבות זאת, פורצים יוכלו לנצל סקריפטים אוטומטיים שיסייעו להעמיס תיבות דואר של משתמשים תמימים ו/או את תיבת המערכת בעצמה. העדר בדיקות האוטומציה (CAPTCHA) עלול גם לאפשר לפורצים להציף את המערכת בתוכן עד לשלב בו לא יישארו למערכת משאבי אחסון לפניות חדשות, מה שעשוי למנוע ממשתמשים לשלוח פניות חדשות, ואף עשוי למנוע מהמערכת לתפקד כראוי באספקטים שונים.

הוכחת קיום ממצא:

העדר הגנות אוטומציה (CAPTCHA) בטופס צור קשר, שתף ותמיכה.



המלצות לתיקון

יש להטמיע הגנות CAPTCHA בכל הטפסים המאפשרים למשתמש לשלוח פניות מצטברות או להעלות תוכן, הגנות אלו כוללות הצגה של תמונה (JPEG) הכוללת אותיות ומספרים לצד המשתמש, ווידוא בצד השרת כי המשתמש הקיש ושלח עם טופס הבקשה את התווים המתאימים לאלו שהוצגו לו בתמונה. יש לייצר את תמונת ה-CAPTCHA המוצגת למשתמש באופן דינאמי לפי ערך תווים אקראי, ולא להשתמש במאגר תמונות מוכן מראש (מכיוון שניתן יהיה למפות מאגר זה), בכדי לממש את בדיקת תקינות הערכים שהוזנו יש לאחסן את ערך התווים לפיו נוצרה התמונה בזיכרון ה-SESSION של המשתמש המצוי בצד השרת, ולהשוות את ערך התווים שהתקבל מצד המשתמש לערך המאוחסן ב-SESSION.

חשוב לציין כי על תמונת CAPTCHA להיות חד פעמית, לאחר כל טעות בהקשת ערך תווים בתמונה יש להחליף תמונה, וכפועל יוצא להחליף את ערכי ההשוואה ב-SESSION המשתמש. כמו כן, על מנגנון ה-CAPTCHA להתגונן מהתקפות OCR (Optical Character Recognition) על ידי הצגת תמונה שתהיה מורכבת לניתוח ממוחשב, אך עדיין תאפשר למשתמש אנושי לזהות את התווים ולהקישם בהצלחה.

4.2. לא קיימת הגנה מפני התקפת Clickjacking

רמת חומרה: ***נמוכה***

סיווג ממצא: *Configuration*

תיאור הבעיה

במהלך המבדק נמצא כי בכותרות המתקבלות מהשרת לא קיימת הגדרה המורה על הדפדפן לבצע הגנה מפני הצגת תוכן באתר מרוחק (iframe) מה שחושף את משתמשי האתר להתקפות מסוג Phishing ו – Clickjacking היות וניתן להציג תכנים של אתר אחים לנשק באתרים מרוחקים ללא כל חסימה מצד הדפדפן. יש לציין כי הגדרות למניעת התקפות מסוג זה מגיעות מהשרת והחסימה בפועל מבוצעת בדפדפן שבצד הלקוח.

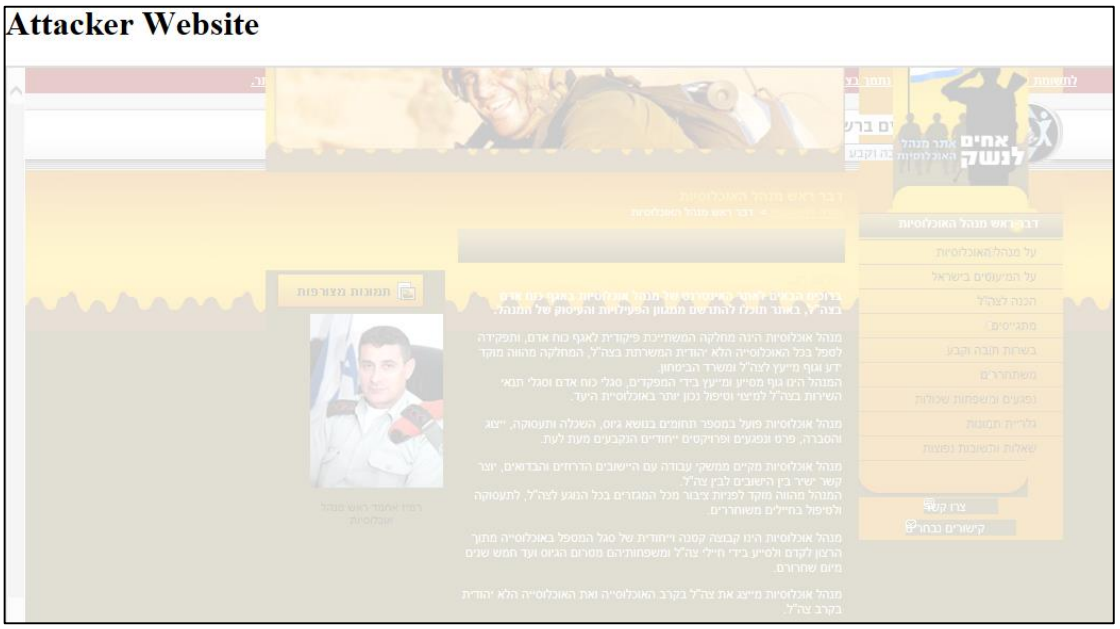
פרטים טכניים

כאשר גולשים לאתר אחים לנשק מתקבלות כותרות מצד השרת אל הדפדפן של הגולש ולפיהן הדפדפן מבצע פעולות שונות בצד הלקוח.

ניתן לראות כי לא מתקבלות כותרות המורות על הדפדפן לבצע הגנה מפני Clickjacking, כגון –X-Frame-Options: deny , ולכן במצב זה ניתן להציג תכנים של אתר אחים לנשק באתר מרוחק ולבצע הונאות שונות למשתמשי האתר באתרים זדוניים.

הוכחת קיום ממצא:

דוגמא 1: הצגת תכנים של אתר אחים לנשק באתר מרוחק



המלצות לתיקון

- יש להגדיר בכותרות שרת ה- IIS את הגדרת ה- X-Frame, בהגדרה זו ניתן לבחור בין אם לאפשר הצגת תכנים תחת אותו דומיין במיקומים שונים בו או לחלופין לחסום זאת לכולם. להלן אפשרויות ההגדרה:

חסימה לגמרי – DENY

מאופשר לאותו דומיין – SAMEORIGIN

מאופשר לכתובת ספציפית - ALLOW-FROM

4.3 שירותים לא מוקשחים חושפים מידע פנימי אודות המערכת

רמת חומרה: נמוכה

סיווג ממצא: *Data Exposure*

תיאור הבעיה

המערכת חושפת מידע אודות התשתית בה היא מאוחסנת כגון פלטפורמת הפיתוח, גרסת ASP.NET וכו'. חשיפת מידע זה מאפשרת לגורם זדוני לאסוף מידע חיוני על המערכת ולמקד את התקפתם. חשיפת המידע עוזרת לתוקפים למצוא פגיעויות ידועות או חדשות אשר קיימות או יימצאו במערכת.

פרטים טכניים

בעת ביצוע פעולות באתר, הכותרות החוזרות לצד המשתמש חושפות מידע אודות גרסת המערכת.

הוכחת קיום ממצא:

זיהוי גרסת המערכת

```
HTTP/1.1 200 OK
Cache-Control: private
Content-Length: 22178
Content-Type: text/html
X-Powered-By: ASP.NET
Date: Wed, 08 Jul 2015 08:07:28 GMT
```

המלצות לתיקון

- יש להקשיח את שרת ה- IIS כך שלא יחשוף את גרסתו ואת הגרסאות של המודולים המותקנים בו.