מבדק חדירות

אתר מילואים אישי
מובייל

צוות אבטחת מידע

ינואר, 2016

תוכן עניינים

1. מאפייני מסמך

מחבר	אודי ברוך
מבקר	
מספר גרסה	2.0
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	07.01.2016	אודי ברוך	דוח ראשון
2.0	07.01.2016	יוגב מזרחי	

הפצה

מ. גרסה	נמענים

2. כללי

2.1 הקדמה

מסמך זה מתאר את ממצאי בדיקת החדירות שבוצעה על אתר מילואים אישי במובייל במהלך חודש ינואר 2016, שארכו כשלושה 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 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.

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
4.1	חשיפת פרטי הזדהות בקוד צד לקוח	**גבוהה**
4.2	חשיפת כתובת של שרת ברשת הפנימית	**בינונית**
4.3	לא קיימת הגנה מפני התקפתClick-jacking	**בינונית**
4.4	שימוש ברכיבים לא מעודכנים	**בינונית**
4.5	דפי בדיקה חושפים מידע פרטי	**בינונית**
4.4	אי טיפול בהודעות שגיאה	**נמוכה**

4.1 חשיפת פרטי הזדהות בקוד צד לקוח

רמת חומרה: ***גבוהה***

סיווג ממצא: *Input and Data Validation*

תיאור הבעיה

המערכת שומרת פרטי הזדהות של משתמש (כנראה מסביבת הבדיקות) באופן גלוי בקובץ קוד בצד לקוח.
כתוצאה מכך, גישה לקובץ זה ע"י משתמש זדוני או משתמש שאינו מורשה לכך, תאפשר לתוקף גישה שאינה מורשת למערכת או חשיפת מידע חיוני העשוי לעזור לתוקף (כמו כן חשיפת מידע פרטי).

פרטים טכניים

במהלך הבדיקה נמצא כי פרטי הזדהות נמצאים באופן גלוי בקובץ JS שנשמר בצד לקוח כהערת מפתח.
גילוי זה עלול להוביל משתמש זדוני לגשת למערכת באופן שאינו מורשה או לחשוף מידע חיוני.

הוכחת קיום ממצא:

המלצות לתיקון

- יש להסיר כל מידע רגיש ופרטי הזדהות בפרט מצד לקוח.
- יש למחוק הערות לא רצויות בעת העלאת גרסה לשרתי ייצור

4.2 חשיפת כתובת של שרת ברשת הפנימית

רמת חומרה: ***בינונית***

סיווג ממצא: *Configuration*

תיאור הבעיה

במהלך המבדק נמצא כי המערכת חושפת כתובת של שרת פנימי.
משתמש זדוני יכול לנצל חשיפה מסוג זה לחקירה והבנה של מבנה הרשת הפנימית (טכנולוגיה ואכיטקטורה).
חשיפה זאת עלולה לעזור למינוף התקפות ממוקדות על שרתים פנימיים.

פרטים טכניים

כאשר גולשים לאתר המערכת, ניתן לראות בתשובות המתקבלות מהשרת Location Header המכיל כתובת של שרת ברשת הפנימית.

הכתובת אשר התגלתה הינה:

192.168.222.10

הוכחת קיום ממצא:

```
+ RFC-1918 IP address found in the 'location' header. The IP is "192.168.222.10".
+ OSVDB-630: IIS may reveal its internal or real IP in the Location header via a request to the /images directory.
The value is "http://192.168.222.10/images/".
```

המלצות לתיקון

יש לבטל את החזרת כתובת ה-IP בתשובה של השרת, מידע על הפתרון:

http://blogs.msdn.com/b/webtopics/archive/2008/11/18/removing-an-iis-server-s-ip-address-from-http-responses.aspx

4.3. לא קיימת הגנה מפני התקפת Click-jacking

רמת חומרה: ***בינונית***

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 האתר באתרים מרוחקים ללא כל חסימה מצד הדפדפן. יש לציין כי הגדרות למניעת התקפות מסוג זה מגיעות מהשרת והחסימה בפועל מבוצעת בדפדפן שבצד הלקוח.

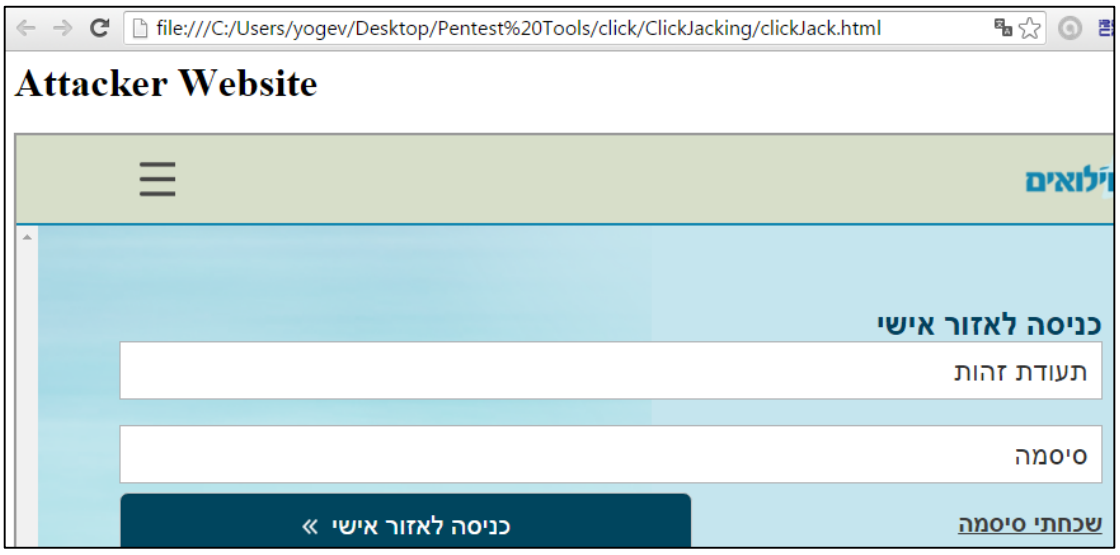
פרטים טכניים

כאשר גולשים לאתר המערכת 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 המערכת באתר מרוחק ולבצע הונאות שונות למשתמשי האתר באתרים זדוניים.

הוכחת קיום ממצא:

הצגת התכנים 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

4.4 שימוש ברכיבים לא מעודכנים

רמת חומרה: ***בינונית***

סיווג ממצא: Implementation

תיאור הבעיה

במהלך המבדק נמצא כי האתר משתמש ברכיב jQuery בגרסה שאינה עדכנית ושקיימות בה בעיות אבטחה. שימוש בספריית jQuery לא מעודכנת חושף את האתר ומשתמשיו לבעיות אבטחה אשר התגלו באותה גרסה מה שעשוי לעזור לגורם זדוני לנצל זאת לצורך התקפות על משתמשי האתר.

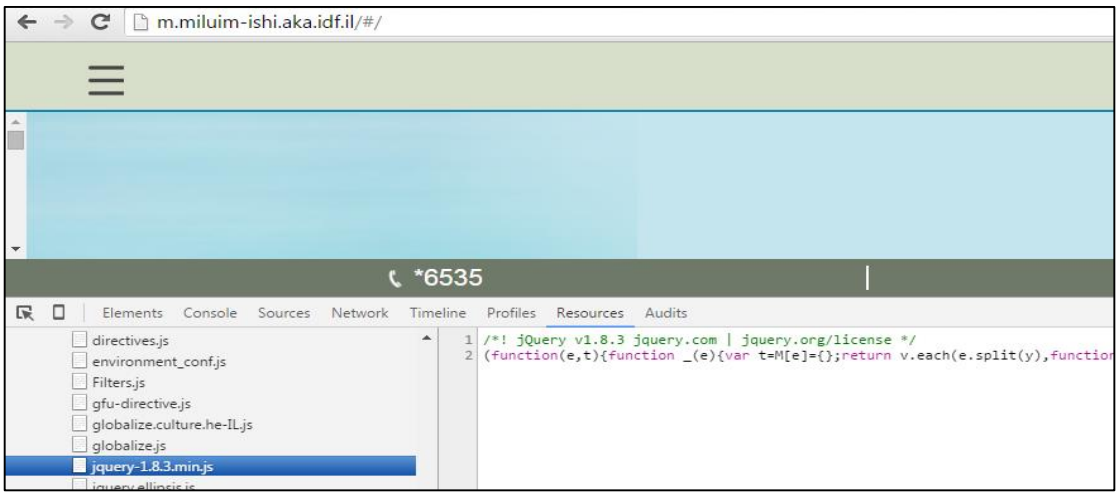
פרטים טכניים

כחלק מבדיקות המערכת נמצא כי נעשה שימוש באתר בספריית jQuery בגרסה ישנה, הגרסה בה נעשה שימוש הינה 1.8.3. גרסה זו חשופה לבעיות אבטחה כגון פגיעות XSS הנקראת "class selector XSS". בקישור הבא ניתן לראות את רשימת הגרסאות הפגיעות לחולשה זו לרבות גרסה 1.8.3 הקיימת באתר:

http://domstorm.skepticfx.com/modules?id=529bbe6e125fac0000000003

הוכחת קיום ממצא:

דוגמא 1: קיום ספריית jQuery לא עדכנית



המלצות לתיקון

יש לבחון שדרוג של כל המודולים והתוספים באתר לגרסאות האחרונות בכדי להוריד את הסיכון לפגיעה במערכת. יש לעדכן לגרסה הכי עדכנית שניתן.

4.5 דפי בדיקה חושפים מידע וגישה למערכת

רמת חומרה: ***בינונית***

סיווג ממצא: *Data Exposure*

תיאור הבעיה

המערכת מכילה קבצי בדיקה שככל הנראה נוצרו בשלב הפיתוח הנגישים למשתמשים אנונימיים. קבצים שאינם רלוונטיים ובייחוד קבצי בדיקה אשר נוצרו בשלב הפיתוח, חושפים בפני גורמים זדוניים מידע חיוני על המערכת ורכיביה, במקרה זה הקבצים חושפים מידע פרטי על אנשי הפיתוח.

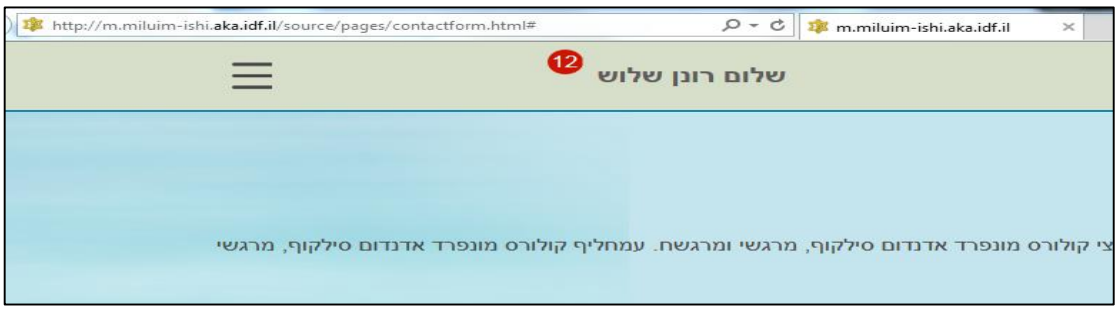
פרטים טכניים

בעת מיפוי הקבצים במערכת ניתן לזהות קבצי HTML אשר ניתן לגשת אליהם ללא צורך בהתחברות למערכת. להלן נתיב לדוגמה:

http://m.miluim-ishi.aka.idf.il/source/pages/contactform.html

עמודים אלה חושפים מידע פרטי על אנשי הפיתוח.

הוכחת קיום ממצא:



טלפון: 03-9999999			
רחוב ברל כצנלסון 28/9, ראשון לציון, 1234567			
סה"כ ימי מילואים לפי שנים	2015	2014	2013
	(120)	(120)	(120)

4.6 אי טיפול בהודעות שגיאה

רמת חומרה: ***נמוכה***

סיווג ממצא: *Configuration*

תיאור הבעיה

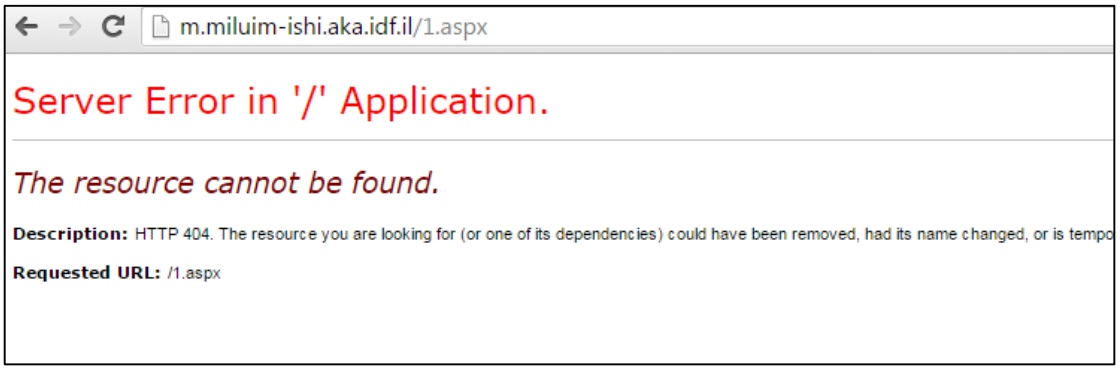
המערכת אינה מטפלת בשגיאות כראוי ועל כן חושפת למשתמש הודעות שגיאה של השרת המכילות מידע שעשוי לחשוף פרטים על המערכת. גורם זדוני עלול לנצל מצב זה של חשיפת המידע הפנימי על המערכת בכדי ללמוד על הרכיבים בה ועל אופי פעולתה. הכרת המערכת הינו שלב מקדים לפעולות התקיפה של גורמים זדוניים ובשלב זה כמה שיותר מידע שנאסף כך יהיה יותר קל לתוקף להשיג את מטרתו ולמצוא חשיפות פנימיות במערכת לרבות חשיפות ידועות הנובעות מהטכנולוגיות עליהן מושתתת המערכת.

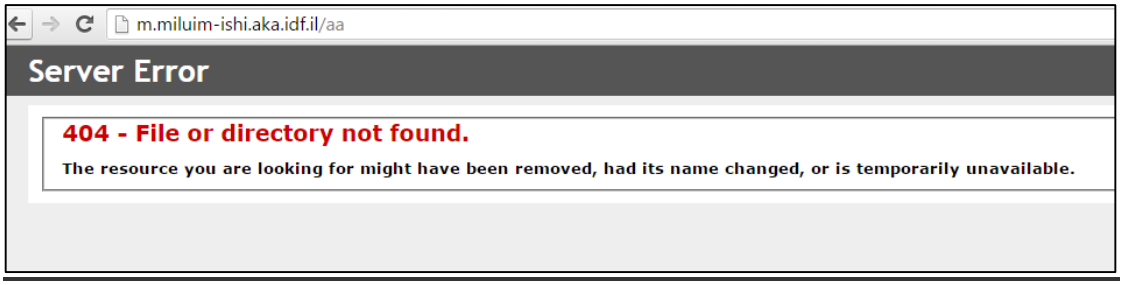
פרטים טכניים

היות ותשתית המערכת אינה מוגדרת ללכוד את כל הודעות השגיאה ולהציג למשתמשים הודעה כללית שאינה חושפת מידע, קיימים מספר מצבים שונים בהם מתרחשת שגיאה החוזרת למשתמש וחושפת את שגיאת השרת. הודעות שגיאה יכולות להתרחש הן מהאפליקציה עצמה והן מהשרת המארח ולכן ברגע שלא מיישמים כראוי את העיקרון של הצגת שגיאה כללית המידע שנחשף מאפשר ללמוד רבות על תשתית המערכת.

הוכחת קיום ממצא:

דוגמאות לשגיאות פנימיות





<u>המלצות לתיקון</u>

- יש ללכוד את כל השגיאות המגיעות מצד האפליקציה ומצד השרת ולהפנות את המשתמש לשגיאה כללית אשר אינה חושפת מידע על השרת.