בדיקת חוסן אפליקטיבית חוזרת – מערכת הגנת הסביבה

עבור

ממשל זמין

בוצע ע"י:

אופק לוי

יועץ אבטחת מידע

חברת 2Bsecure בע"מ

רח' הערבה 3, קריית שדה התעופה. טלפון:03-6492007 פקס: 03-6492008
דוא"ל: info@2bsecure.co.il. אתר: www.2bsecure.co.il

תוכן עניינים

לכבוד: מר. אברהם זרוק **תאריך:** **24/12/2014**

הנדון: בדיקת חוסן אפליקטיבית – מערכת הגנת הסביבה

פרק א' – תקציר מנהלים

כללי

בחודש דצמבר 2014 זומנה חברת 2bsecure לבצע בדיקה אפליקטיבית חוזרת למערכת הגנת הסביבה. הבדיקה המקורית בוצעה בחודש נובמבר 2014. הבדיקה התבצעה על המערכת בכתובת הבאה:

http://hagnas.atal.idf.il

סיכום

בבדיקה נמצא כי חלק גדול ממצאי המערכת לא תוקנו באופן מספק.
כתוצאה, המערכת נמצאת בסיכון **גבוה** למתקפות אפליקטיביות. מומלץ לתקן את ממצאי הבדיקה ולבצע בדיקה חוזרת בטרם הפצת המערכת.

טבלת סטטוס ממצאים

לפניך טבלת סיכום הכוללת את סטטוס הממצאים.

מס	שם הממצא	חומרה	סטטוס	הסבר
.1	שימוש ברכיבי תוכנה פגיעים	**גבוהה**	**לא תוקן**	
.2	משתנה ViewState אינו מוצפן	**בינונית**	**לא תוקן**	במספר מקומות נמצא כי הוא מוצפן אך לא בכל המערכת.
.3	חשיפת גרסת השרת	**נמוכה**	**לא תוקן**	
.4	שימוש בשם ברירת מחדל של ה cookie	**נמוכה**	**תוקן**	

כמו כן, במהלך הבדיקה החוזרת נמצא במערכת ממצא נוסף:

1. חשיפת כתובות דואר אלקטרוני

תיאור האיום:

האפליקציה חושפת, אם בקוד המקור או פשוט כתצוגה על מסך המשתמש, כתובות הדואר האלקטרוני של עובדי הארגון כתובות אילו עשויות לחשוף מידע שימושי לתוקף.
תוקף אלול לעשות שימוש בכתובות אילו תוך מתקפה מסוג הנדסה חברתית, הכתובות עשויות לייצג שמות משתמשים בארגון, ובנוסף ניתן לתקוף משתמש ספציפי על ידי הצפת תיבת המייל שלו.

רמת סיכון:

בינונית

סיווג STRIDE:

Information Disclosure - חשיפת מידע

טכניקת המתקפה:

תוקף יכול בקלות לשלוף את כתובות הדואר האלקטרוני אשר מוטמעות באתר ולעשות בהן שימוש זדוני לתקיפת האתר או הארגון.
להלן חלק מכתובות הדואר החשופות:

anders@nomadiz.se
apaella@gmail.com
arturas.paleicikas@metasite.net
arturas@avalon.lt
cloudream@gmail.com
dedenf@gmail.com
deletestuff@gmail.com
flakron@gmail.com
harrikilpio@gmail.com
haukur@eskill.is
ionut.g.stan@gmail.com
jacek.wysocki@gmail.com
jaka@kubje.org
jmowla@gmail.com
joan.leon@gmail.com
jquerycalendar@spam.raszi.hu
kara@karalamalar.net
kbwood@virginbroadband.com.au

אמצעי נגד:

1. נדרש להסיר כתובות דואר אלקטרוני אשר לא הכרחיות.
2. נדרש להחליף את כתובות הדואר האלקטרוני הפרטיות לכתובות גנריות.

פרק ב' – פרטי הממצאים שלא תוקנו

מספרי הממצאים בפרק זה תואמים את מספרי הממצאים במסמך המקורי ולכן ייתכן מאוד שהמספרים אינם רציפים.

1. שימוש ברכיבי תוכנה פגיעים

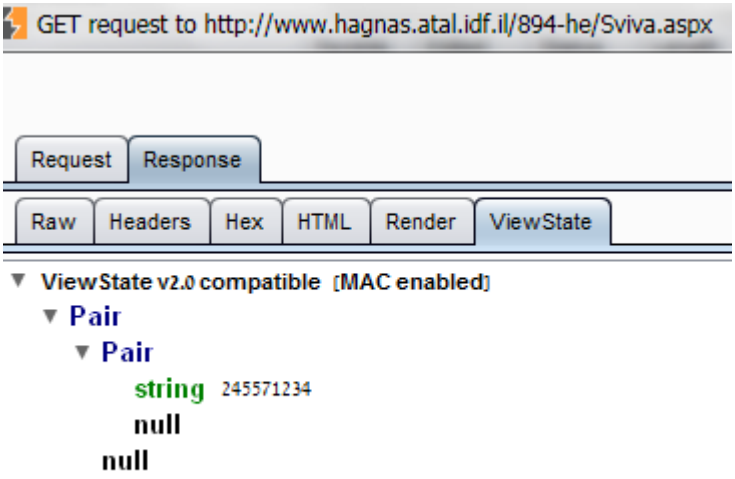
להלן צילום מסך מהבדיקה החוזרת:

אמצעי נגד:

1. מומלץ לשדרג את גרסת השרת.

2. משתנה ViewState אינו מוצפן

להלן צילום מסך של משתנה ה ViewState כפי שנמצא במהלך הבדיקה החוזרת:



אמצעי נגד:

1. מומלץ להצפין את משתנה ה View State -באמצעות ההצהרה המובנת של .NET. בראש כל דף:

```
<%@Page ViewStateEncryptionMode="Always" %>
```

2. מומלץ להשתמש בפרמטר ViewStateUserKey כדי למנוע מתקפות.CSRF

למידע נוסף בנושא:

http://msdn.microsoft.com/en-us/library/system.web.ui.page.viewstateuserkey(v=vs.110).aspx

3. חשיפת גרסת השרת

להלן צילום מסך של חשיפת גרסת השרת:

אמצעי נגד:

1. מומלץ לדאוג להסתיר את המידע בשרת האפליקציה. תהליך מפורט בכתובת:

http://blogs.msdn.com/b/varunm/archive/2013/04/23/remove-unwanted-http-response-headers.aspx