תקציר בדיקת הרגרסיה השנייה באתר מפקדים-מילואים

כתב:

אייל גרינברג

מסמך זה מפרט את הסטטוס של תיקוני הפערים כפי שנבדקו בתאריך 6.11.2014 בממשל זמין. בנוסף, לאור דרישות שקיבל המדור, מצויינת דעתנו לגבי דחיפות הממצאים בדו״ח בדיקת החדירות- האם הם צריכים לעכב עליה של האתר. בסוף מסמך זה מפורטות דרישות מחברת CA לצורך השלמת תהליך התיקונים.

שימו לב: מספר הממצאים על פי הדו״ח הסופי שנשלח בשביעי לאוגוסט.

סיכום הממצאים:

4.1: תוקן (מעכב)

4.2: תוקן על ידי הסרת כלל הדפים שלא נדרשים, בפרט הדפים הפגיעים. (מעכב)

4.3: תוקן (מעכב)

4.4: בתהליך - ממשל זמין ידווחו כי משתמשי מנהלנים אישיים פוצלו למשתמשי Front ו-Back. קיים משתמש Admin משותף לצורך משימות מתוזמנות ב-Back שכותבות ל-Share ב-Front, על ממשל זמין בעזרת Matrix לרדד את ההרשאות שלו. (מעכב)

4.5: תוקן (מעכב)

4.6: תוקן (מעכב)

4.7: תוקן- הובהר כי לא תעשה גלישה מתוך הדומיין לאתר מלבד לתקלות מסוימות בלבד. (מעכב)

4.8: לא תוקן, התיקון שהוצע שובר פונקציונליות באתר כיוון ש-sp צריך להציג frame מתוך owa. (מעכב)

4.9: רוב הפערים הקריטיים תוקנו, מלבד הבאים: בתהליך- נושא Host Firewall אושר על ידי ראש צוות אבטחת מידע בממשל זמין, רידוד הרשאות בשרתים נכנס לתהליך תיקונים, הצפנת קבצי קונפיגורציה נכנס לתהליך. לא תוקן - נעשה ניסיון לרדד את הרשאות ה-Apache Tomcat של Siteminder ללא הצלחה. יש לקבל התייחסות מ-ca מדוע יש צורך בהרשאות Local Admin למוצר. לא ניתן לשדרג את שרת Tomcat על פי טענת נציג CA. (מעכב)

4.10: תוקן (מעכב)

4.11: לא תוקן, חלק מתשתית KS. ראש צוות אבטחת מידע בממשל זמין דורש לתקן. (לא מעכב)

4.12: בתהליך - ראש צוות אבטחת מידע בממשל זמין ירכוש שרת הלבנה נפרד. ממשל זמין ידווחו על סיום. (מעכב)

4.13: בבדיקה מול matrix. (מעכב)

4.14: לא תוקן - נחוץ לתהליך אפליקטיבי באתר של העתקת קבצים מ-Back ל-Front. (לא מעכב)

4.15: תוקן (מעכב)

4.16: תוקן (מנגנון הרשאות חלש בפורום מפקדים) (מעכב)

4.17: לא תוקן, יש להדגיש שהמדיניות הלקויה הוגדרה על ידי מחב״ם. (מעכב)

4.18: תוקן, נמנעת גישה לurlים המסתיימים ב-doc, ppt וכדומה ולכן הבעיה המתוארת בדו״ח לא חשופה. (מעכב)

4.19: תוקן (מעכב)

דרישות מ-CA בנוגע לפערים שלא תוקנו ב-Siteminder:

* בהקשר לממצא 4.8: יש להוציא תיקון לקוד הבעייתי, למשל כפי שמתואר כאן:

<https://www.owasp.org/index.php/Clickjacking_Defense_Cheat_Sheet#Best-for-now_Legacy_Browser_Frame_Breaking_Script>

* בהקשר לממצא 4.9: יש לקבל מדיניות עדכונים וכיצד יש לטפל בפערי אבטחה הקיימים ושעלולים להתגלות בגרסאות הנוכחיות של Apache Tomcat בשרתי ה-Siteminder. בנוסף, יש לקבל התייחסות אילו פעולות אדמיניסטרטיביות שירול ה-Apache Tomcat מבצע, ואם הוא אינו מבצע כאלו כיצד יש לרדד את ההרשאות שלו.