**תקציר בדיקת הרגרסיה באתר מפקדים**-**מילואים**

כתבו:

אייל גרינברג

ברק ארקיס

בתאריך 2.11.2014, ביצע מדור 21 סקר בממשל זמין לבדיקת סטטוס התיקונים בעקבות בדיקת החדירות של אתר מילואים-מפקדים. מובאים מטה ממצאי הסקר. חומרת הממצאים כמפורט בדו״ח המקורי.

יש לציין כי אף ממצא שקשור ל-CA Siteminder, ובפרט ממצאים קריטיים, לא תוקנו.

# **סיכום הממצאים**:

4.1: תוקן

4.2: לא תוקן

4.3: תוקן חלקית, אך יש להגדיר את העוגיה כ-secure (לא נבדק בבדיקת החדירות כיוון שהאתר הוגדר ללא SSL)

4.4: תוקן חלקית, כמות ה-DA קטנה בכחצי, אך עדיין מחוברים לשרתים. בנוסף, ישנם משתמשים local admin גם על שרתי frontend וגם על שרתי backend.

4.5: תוקן

4.6: תוקן חלקית, ממשקים רבים עדיין חשופים, הממשק של Tomcat והדפים בתיקיית example

4.7: לא תוקן, הגישה עדיין אפשרית

4.8: לא תוקן

4.9: תוקן חלקית, שירותים בהרשאות גבוהות, Host Firewall מכיל חוקי any-any-any ועוד.

4.10: לא תוקן, המסמך עדיין קיים בשרת

4.11: לא תוקן, חלק מהתשתית.

4.12: לא תוקן

4.13: בבדיקה מול matrix

4.14: לא תוקן

4.15: תוקן חלקית, אין קטעי קוד בהודעות השגיאה אך יש call stack

4.16: לא תוקן, יש להדגיש שהמדיניות הלקויה הוגדרה על ידי מחב״ם.

4.17: לא רלוונטי, הבעיה לא קיימת (טיוטה)

4.18: (4.17 בגרסא הסופית) - לא תוקן

4.19: (4.87 בגרסא הסופית) לא נבדק כתוצאה מתקלה באתר בזמן הבדיקה