עדכון חדשות סייבר יומי 14/01/18

עדכון זה ניתן כשירות ומבוסס על לקט פרסומים גלויים.

הפרסומים מובאים בשם אומרם ואינם משקפים את עמדת המערך ו/או פעולותיו.

בעולם

1. האקר הצליח לפרוץ לרשת של בית חולים באינדיאנה ולהתקין פוגען כופר. הוא דרש תשלום בביטקוין. הנהלת בית החולים החליטה לכבות את כלל הרשת כדי למנוע את התפשטות הפוגען. טרם ידועים פרטים נוספים (hackread).

טכנולוגי

2. חברת Trend Micro איתרה קמפיין חדש של קבוצת התקיפה Fancy Bear, המכונה גם Pawn Storm, במסגרתו הוקמו אתרי דיוג בניסיון לדלות מידע מהסנאט האמריקני. אינדיקטורים רלוונטיים בקישור (trendmicro).

3. חברת AMD מאשרת כי פגיעות Spectre רלוונטית למעבדים מתוצרתה. הפגיעות הראשונה (CVE-2017-5753) תטופל באמצעות עדכוני מערכת הפעלה. הפגיעות השנייה (CVE-2017-5715) תטופל באמצעות עדכון אופציונלי למעבדים בצירוף עדכוני מערכת הפעלה, אם כי החברה טוענת כי הארכיטקטורה של המעבדים מקשה על מימוש התקיפה. החברה הבהירה בנוסף כי פגיעות Meltdown לא משפיעה על מעבדיה לאור הארכיטקטורה שלהם. מיקרוסופט צפויה לחדש את תהליך העדכונים למחשבים בעלי מעבדי AMD ישנים במהלך שבוע זה (amd ו-securityweek).

4. חוקרים גילו פגיעות נוספת בטכנולוגיית הניהול מרחוק (AMT) של מעבדים מתוצרת Intel, ללא קשר לדיווחי העבר על הפגיעויות בטכנולוגיה זו או לפגיעויות האחרונות בנושא המעבדים. הפגיעות היא ברכיב Management Engine BIOS Extension, אך דורשת נגישות פיזית לביצוע החלק הראשון בתקיפה (fsecure).

5. חוקרי חברת צ'ק פוינט איתרו קוד זדוני שהוסווה בתוך 60 אפליקציות בחנות של Google. במסגרת התקיפה, קופצות פרסומות של תכנים למבוגרים, נעשה ניסיון לעודד להתקנת שירותי פרימיום ועוד. לדברי החברה, היקף ההורדות של אפליקציות אלו נע בין 3 ל-7 מיליון (checkpoint).

6. במרבית האפליקציות הסלולריות בתחום ה-SCADA נמצאו פגיעויות אבטחה שעלולות להשפיע על תהליך הייצור. כך נחשף במחקר של חברות IOActive ו-Embedi. במסגרת המחקר נבדקו אפליקציות של 34 יצרנים (ioactive).

עדכוני אבטחה

7. חברת Juniper פרסמה עדכוני אבטחה למגוון מוצרים (us-cert).

כתובת לקבלת דואר: משרד ראש הממשלה, רח' קפלן 3, ירושלים
טלפון 03-7450811, פקס 03-7450822