סייבר ישראל
Cyber Israel

בלמ״ס

TLP : לבן

27 יוני 2018
י״ד תמוז תשע״ח
סימוכין : ב-ס-649

פגיעות ב- Acrobat Reader מנוצלת בפועל לתקיפות

תקציר

לאחרונה דווח על ניצול בפועל של פגיעות בתוכנת Acrobat Reader של חברת Adobe.
לפגיעות קיים PoC ברשת. מומלץ להתקין את עדכוני האבטחה הרלוונטיים בהקדם.

פרטים

הפגיעות (CVE-2018-4990) מאפשרת הרצת קוד מרחוק (RCE). הפעלת הפגיעות מתאפשרת באמצעות קוד JavaScript זדוני שמוטמע בתוך קובץ PDF. עם זאת, כדי לעקוף את מנגנון ה-Sandbox שקיים בגרסאות האחרונות של התוכנה, יש צורך בניצול של פגיעות נוספת לטובת התקיפה.
לפי הדיווח, הפגיעות הנוספת המנוצלת במקרה זה היא במערכת ההפעלה Windows (CVE-2018-8120) ומאפשרת העלאת הרשאות ומעקף של מנגנון ה-Sandbox.

דרכי התמודדות

Adobe הוציאה עדכוני אבטחה כמענה לפגיעות זו. ניתן להוריד את העדכונים כאן.
עדכון לפגיעות ב-Windows, ניתן להוריד כאן.
מומלץ לבחון את העדכונים במערכותיכם, ולהתקינם בהקדם האפשרי.
מומלץ לנטרל הפעלת קוד JavaScript במסמכי PDF, בפרט כאלו שמקורם ברשת האינטרנט.
ניתן לבצע זאת באמצעות בחירה ב :

Edit > Preferences > Categories > JavaScript

כדי לנטרל השימוש ב- JavaScript יש **לבטל הבחירה** באפשרות

Enable Acrobat JavaScript

לכל מידע נוסף ניתן לפנות אלינו. במידה שעלו ממצאים בבדיקתכם, נבקש לקבל היזון חוזר.

הערה: שיתוף מידע עם ה-

בברכה,
CERT-IL
טל*9344:
team@cert.gov.il

Qualified by a Certificate Authority