31 יולי 2019
כ"ח תמוז תשע"ט
סימוכין: ב-ס-978

פגיעויות קריטיות ב- iOS של אפל מאפשרות הרצת קוד מרחוק ללא מעורבות המשתמש

תקציר

1. לאחרונה נחשף כי במערכת ההפעלה iOS של אפל, קיימות מספר פגיעויות קריטיות אשר חלקן מאפשרות הרצת קוד מרחוק ללא מעורבות של המשתמש.
2. הפגיעויות מאפשרות לתוקף לשלוח הודעות iMessage לנתקף, והקוד העוין יבוצע כשהמשתמש יפתח את ההודעה ויצפה בה, ללא צורך בפעולה נוספת מצדו.
3. מומלץ להתקין את גרסת מערכת ההפעלה העדכנית ביותר, 12.4, הכוללת עדכוני אבטחה עבור פגיעויות אלו.

פרטים

1. מתוך 6 הפגיעויות שפורסמו, 4 מאפשרות הרצת קוד מרחוק ללא מעורבות המשתמש. 2 הפגיעויות הנותרות מאפשרות דלף מידע, וקריאת קבצים מהמכשיר המותקף, גם במקרה זה ללא מעורבות המשתמש.
2. פורסמו מידע טכני וקוד הדגמה ל- 5 מתוך 6 הפגיעויות. המידע עבור הפגיעות האחרונה לא פורסם משום שהעדכון כבל הנראה לא פותר את הבעיה באופן מלא.
3. הפגיעויות המאפשרות הרצת קוד מרחוק הן:

CVE-2019-8641, CVE-2019-8647, CVE-2019-8660, CVE-2019-8662

4. הפגיעויות המאפשרות דלף מידע הן:

CVE-2019-8624, CVE-2019-8646

דרכי התמודדות

1. מומלץ להתקין בהקדם האפשרי את הגרסה העדכנית ביותר של מערכת ההפעלה – 12.4. ניתן למצוא הנחיות מפורטות באן.

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

מקורות

1. https://support.apple.com/en-il/HT201222
2. https://support.apple.com/en-us/HT210346
3. https://support.apple.com/en-il/HT204204
4. https://www.zdnet.com/article/google-researchers-disclose-exploits-for-interactionless-ios-attacks/

שיתוף מידע עם הCERT הלאומי איננו מחליף חובת דיווח לגוף מנחה כלשהו, במידה שהתגלה צורך כזה

בברכה,
CERT-IL