

10 מאי 2020  
ט"ז אייר תש"פ  
סימוכין: ב-ס-1077

## פגיעות בפלאפונים מתוצרת סמסונג

### תקציר



לאחרונה הוציאה חברת סמסונג עדכון אבטחה לפגיעות בפלאפונים מתוצרתה. הפגיעות קיימת החל משנת 2014, ועלולה להיות מנוצלת לצורך הרצת קוד מרחוק על ידי תוקף, ללא צורך בפעולה כלשהי מצד המשתמש. מומלץ להשתמש בפונקציית עדכון מערכת ההפעלה של המכשירים הרלוונטיים, ולעדכןם בהקדם האפשרי.

### פרטים



1. הפגיעות זוהתה על ידי חוקר החבר ב-Project Zero של חברת גוגל.
2. הפגיעות קיימת במכשירי אנדרואיד גרסאות 8, 9, 10, מתוצרת **סמסונג בלבד**.
3. מקור הפגיעות בספריה בשם **Quram**, המשמשת להצגת קבצים גרפיים. משלוח קובץ ספציפי בפורמט **Qmage (QMG)** עלול לאפשר לתוקף הרצת קוד מרחוק ללא מעורבות מצד המשתמש.
4. לדברי החוקר, תקיפה מוצלחת תדרוש משלוח של בין 50 ל-300 הודעות **MMS** המכילות קבצים גרפיים. להערכתו, משך הזמן לביצוע התקיפה ינוע סביב 100 דקות.

**דרכי התמודדות**

1. מומלץ להשתמש במנגנון עדכון מערכת ההפעלה המותקן במכשיר, על מנת לבדוק אם עדכונים זמינים עבור המכשיר שברשותכם.
2. זמינות העדכונים תלויה לעיתים לא רק ביצרן, אלא גם במפעילת הרשת שלכם.
3. אם קיים עדכון זמין, מומלץ להתקינו בהקדם האפשרי. אם העדכון עדיין לא זמין, מומלץ לבדוק זמינותו באופן עיתי.

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

**מקורות**

1. <https://www.tripwire.com/state-of-security/security-data-protection/six-years-samsung-smartphone-users-risk-critical-security-bug-patch-now/>
2. <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-8899>
3. <https://bugs.chromium.org/p/project-zero/issues/detail?id=2002>

שיתוף מידע עם ה-CERT הלאומי אינו מחליף חובת דיווח לגוף מנחה כלשהו, ככל שחלה על הגוף חובה כזו. המידע נמסר כפי שהוא (as is), השימוש בו הוא באחריות המשתמש ומומלץ להיעזר באיש מקצוע בעל הכשרה מתאימה לצורך הטמעתו.



בברכה,  
CERT-IL