# הזלגת זיכרון ב-Nexus 5x דרך USB

מאת רועי חי

## הקדמה

תקיפה פיזית של מכשירים סלולריים הינה סיכון שהיצרניות מתייחסות אליו בכובד ראש. לתקיפה יכולות להיות מטרות שונות - מגניבה מוצלחת ועד פורנזיקה. דוגמאות לא חסר, ואחת הבולטות מביניהן היא ללא ספק מקרה סן ברנרדינו, שבו ה-FBI ביקש מ-Apple "לפתוח" עבורו את מכשיר ה-iPhone של המפגע.

הכלל הוא שבהינתן נגישות פיזית של תוקף למכשיר נעול, לא אמורה להיות לו שום אפשרות להזליג מידע רגיש של הקורבן. כמובן שזו בעיה קשה, ולכן יש מספר מנגנונים על מנת לממשה, הן ב-iOS והן ב-Android. מאמר זה הוא על חולשה באנדרואיד, ולכן אתמקד בו.

מנגנוני ההגנה באנדרואיד סביב תקיפות פיזיות הם מגוונים, וכוללים את היכולות הבאות:

1. Full Disk Encryption - data/ (שמכיל מידע אישי של המשתמש) מוצפן עם מפתח שתלוי בסוד (סיסמא \ קוד \ תבנית) שהמשתמש מספק בזמן עליית המערכת, Salt ומידע שקיים ב-TEE ואינו נגיש באופן אפליקטיבי.
2. נשים לב שתיאורטית, אם זו היתה ההגנה היחידה בלבד, התוקף היה יכול לגשת פיזית ובאופן זמני למכשיר, להחליף את מערכת ההפעלה במערכת זדונית, ולהחזיר את המכשיר לקורבן. בשלב זה התוקף פשוט היה מחכה למידע שיהיה זמין (לא מוצפן). כדי להתמודד עם בעיה זו, מכשירי אנדרואיד נעולים לא מאפשרים לצרוב מערכת הפעלה חדשה, מבלי לעשות להם קודם unlock, דבר הגורר Factory Reset ומחיקת מידע המשתמש.
3. כמו כן, קיים מנגנון בשם Verified Boot, אשר מונע שימוש במערכת הפעלה זדונית, במידה והתוקף הצליח איכשהו כן לשנות את מערכת ההפעלה. מכשירים נעולים יסרבו לרוץ, מכשירים בלתי נעולים יתריאו מיד למשתמש.
4. Factory Reset Protection (FRP) - נועד לא לאפשר לגנבים לעשות Factory Reset למכשיר, ובכך למנוע את כדאיות הגניבה.

אבל מה עם **הזיכרון**? מה מונע מהתוקף להעתיק את זיכרון המכשיר, שבאופן כמעט ודאי מכיל מידע רגיש?

השאלה הזו נשאלה ע"י מספר חוקרים בעבר, ולכן לא מפתיע שניתן למצוא מספר מחקרים בנושא. (למשל: FROST).

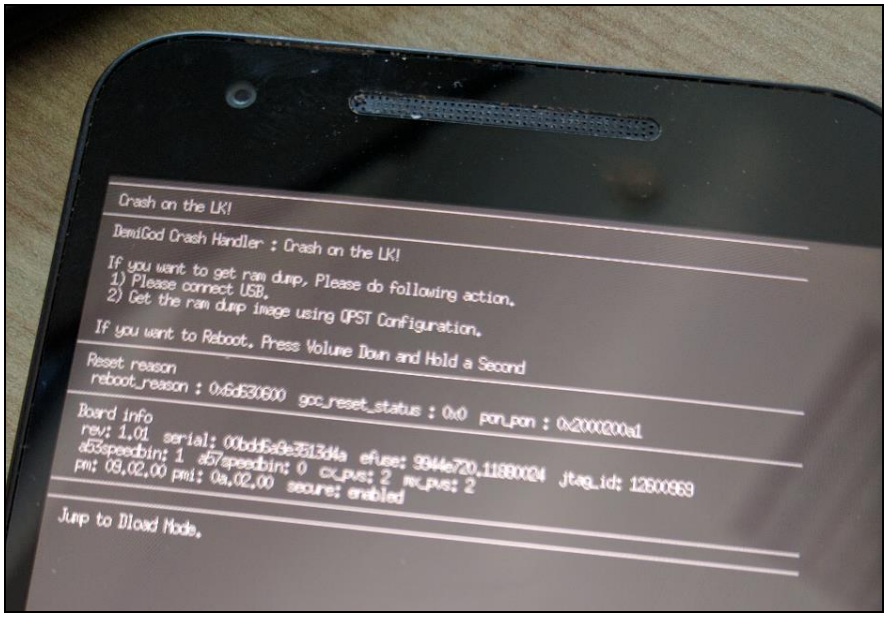
## הפגיעות

לאחרונה הצוות שלי, IBM X-Force Application Security, גילה חולשה, אשר לא תועדה מעולם, בגירסאות ישנות של ה-bootloader של Nexus 5X. החולשה איפשרה לתוקף פיזי "לשאוב" את כל זיכרון המכשיר, אפילו אם הוא נעול, דרך USB. את התקיפה עצמה ניתן לבצע בשניות ספורות, ללא שימוש בכלים מיוחדים - לכן ניתן לבצעה גם עם נגישות זמנית בלבד למכשיר. כמו כן, בתנאים מסויימים היא ניתנת לניצול גם ע"י שימוש במטען זדוני. (וקטור זה דורש ש-ADB יהיה דלוק על המכשיר, ושהקורבן יאשר למטען להתחבר.)

התקיפה מתחילה בכך שהתוקף מרסט את המכשיר למצב מיוחד של ה-bootloader, שחושף ממשק, דרך USB, בשם fastboot. ממשק זה במכשירים בלתי-נעולים מאפשר בין היתר לצרוב מערכת הפעלה חדשה, אולם במכשירים נעולים הוא אמור להיות די אנמי, ולא לאפשר לבצע שום שינוי במערכת ההפעלה, ו/או לגנוב מידע רגיש.
להפתעתנו גילינו פקודה די מעניינת, הזמינה במכשירי Nexus 5X בלבד:

```
fastboot oem panic
```

בעזרת פקודה זו ניתן לכפות קריסה ב-bootloader:



הקריסה עצמה כמובן שהאירה את עינינו, אולם היא אינה בעייתית כשלעצמה. מה שכן בעייתי היא ההודעה הבאה:

> "If you want to get ram dump, Please do the following action,
> 1) Please connect USB
> 2) Get the ram dump image using QPST Configuration."

זו כבר פגיעות! בגרסאות הפגיעות של ה-bootloader, ברגע שהאחרון קורס, הוא חושף ממשק סריאלי מעל USB, אשר מאפשר לתוקף לשאוב את כל זכרון המכשיר, בעזרת כלים כגון QPST Configuration.

כדי להוכיח את חומרת הפגיעות, שיניתי את סיסמת המכשיר שברשותי ל - buggybootload3r, וחיפשתי אותה בזיכרון שהדלפתי:

```
> hexdump DDRCS0_0.BIN | grep -10 bootloa
2675d060: 6f 00 69 00 64 00 2e 00 - 73 00 65 00 72 00 76 00 o.i.d...s.e.r.v.
2675d070: 69 00 63 00 65 00 2e 00 - 67 00 61 00 74 00 65 00 i.c.e...g.a.t.e.
2675d080: 6b 00 65 00 65 00 70 00 - 65 00 72 00 2e 00 49 00 k.e.e.p.e.r...I.
2675d090: 47 00 61 00 74 00 65 00 - 4b 00 65 00 65 00 70 00 G.a.t.e.K.e.e.p.
2675d0a0: 65 00 72 00 53 00 65 00 - 72 00 76 00 69 00 63 00 e.r.S.e.r.v.i.c.
2675d0b0: 65 00 00 00 00 00 00 00 - 3a 00 00 00 00 0d c4 b6 e.............
2675d0c0: 6d 42 cd 0a b1 00 00 00 - 00 00 00 00 00 00 00 00 mB..............
2675d0d0: 00 00 00 00 00 92 86 33 - e3 79 92 8b b7 d4 77 f5 .......3..y....w.
2675d0e0: 94 7f d0 2b fb b8 6e cc - 98 3b 9a a7 0d 7c 60 f6 .....n.........
2675d0f0: d7 70 68 c2 14 01 00 00 - 0f 00 00 00 62 75 67 67 .ph.........bugg
2675d100: 79 62 6f 6f 74 6c 6f 61 - 64 33 72 00 62 75 67 67 ybootload3r.bugg
```

כפי שניתן לראות, הסיסמא מופיעה ב-dump! ברגע זה, התוקף הפיזי יכול לעלות את המכשיר, להתחזות לקורבן, ולגשת למידע פרטי ששמור ב-data/.

את הפגיעות דיווחנו כמובן ל-Google. הם אישרו על דבר קיומה, ושהיא תוקנה בגירסה MHC19J 6.0.1 אשר שוחררה במרץ 2016. פרטים נוספים ניתן למצוא בבלוג של IBM Security.