03 נובמבר 2019
ה' חשון תש"פ
סימוכין:ב-ס-1007

פגיעות Zero Day בדפדפן כרום עלולה לאפשר הרצת קוד מרחוק

תקציר

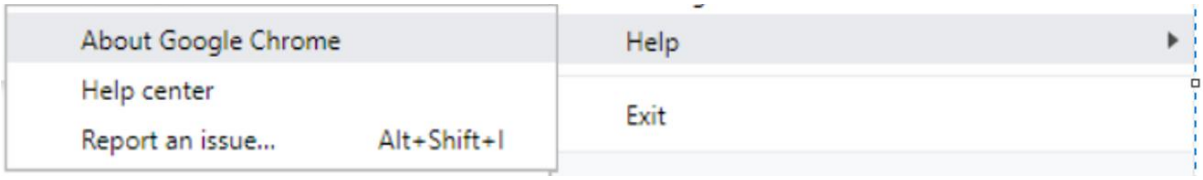
לאחרונה דווח על 2 פגיעויות בדפדפן כרום, העלולות לאפשר לתוקף הרצת קוד מרחוק.
על פי הדיווח, אחת מן הפגיעויות נוצלה בפועל על ידי תוקפים, טרם הוצאת עדכון האבטחה על ידי היצרן (Zero Day Vulnerability).
מומלץ להתקין בהקדם את עדכון האבטחה הרלוונטי.

פרטים

1. הפגיעויות קיימות בגרסאות הדפדפן הקודמות לגרסה 78.0.3904.87, עבור מערכות ההפעלה Linux, Mac, Windows.
2. 2 הפגיעויות מקורן בטעות בניהול הזיכרון המכונה Use After Free (UaF), אשר עלולה לאפשר הרצת קוד מרחוק על ידי התוקף.
3. הפגיעות הראשונה מזוהה כ- CVE-2019-13721, ומקורה ברכיב המאפשר הצגת קבצי PDF על ידי הדפדפן (PDF generation and rendering library - PDFium).
4. הפגיעות השנייה מזוהה כ- CVE-2019-13720, ומקורה ברכיב האודיו של הדפדפן.
5. דווח כי פגיעות זו הייתה בשימוש לתקיפת משתמשים באתר חדשות בשפה הקוריאנית, בשיטה המכונה Watering Hole Attack, בה מודבק האתר בקוד זדוני אשר מופעל בדפדפני המשתמשים הניגשים לאתר. התקיפה הנ"ל גרמה להורדת פוגענים לעמדת המשתמש.

דרכי התמודדות

1. מומלץ לבחון עדכוני תוכנה במערכות ניסוי, טרם הטמעה במערכות ייצור.
2. משתמשים פרטיים, מומלץ לוודא עדכון הדפדפן לגרסה העדכנית (78.0.3904.87) באמצעות בחירה בתפריט Help -> About Google Chrome.



3. משתמשים ארגוניים, מומלץ לעדכן הדפדפן באמצעות המערכות הארגוניות לעדכון תוכנה.
4. להתרעה זו מצורף קובץ מזהים. מומלץ לנטרם במערכות הארגוניות.

מקורות

1. https://chromereleases.googleblog.com/2019/10/stable-channel-update-for-desktop_31.html
2. https://www.us-cert.gov/ncas/current-activity/2019/10/31/google-releases-security-updates-chrome
3. https://www.cisecurity.org/advisory/multiple-vulnerabilities-in-google-chrome-could-allow-for-arbitrary-code-execution_2019-118/
4. https://securelist.com/chrome-0-day-exploit-cve-2019-13720-used-in-operation-wizardopium/94866/

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

בברכה,
CERT-IL