



22 אפריל 2020
כ"ח ניסן תש"פ
סימוכין: ב-ס-1062

פגיעויות קריטיות בשני מוצרים פופולריים

תקציר



לאחרונה דווח על פגיעויות קריטיות בשני מוצרים פופולריים: דפדפן כרום ותוכנת אופיס. מומלץ לבחון העדכונים ולהתקינם בהקדם האפשרי.

פרטים



1. הפגיעות בדפדפן כרום מקורה במצב המכונה **Use After Free (UAF)** ברכיב זיהוי הדיבור, העלול לאפשר לתוקף מניפולציות שונות בזיכרון, עד אפשרות להרצת קוד מרחוק.
2. גרסאות הדפדפן לפני 81.0.4044.113 פגיעות.
3. הפגיעות קיבלה את הזיהוי **CVE-2020-6457**.
4. הפגיעויות בתוכנת אופיס (ובתוכנת **Paint 3D**), מקורה ברכיב של חברת **Autodesk** המאפשר לתוכנה הצגת מודלים של תוכנת **Autodesk** בתלת-מימד. תוקף השולח קובץ ספציפי עלול להפעיל פגיעות זו ולהריץ קוד מרחוק בהרשאות המשתמש.
5. הפגיעויות קיבלו את הזיהוי **CVE-2020-7080->7085**.

דרכי התמודדות

1. לקוחות פרטיים - מומלץ לבדוק האם תוכנות אלו כבר עודכנו, ואם לא, ליזום עדכון בהקדם האפשרי.
2. ארגונים - מומלץ לבחון העדכונים במערכותיכם ולהתקינם בהקדם האפשרי.

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

מקורות

1. <https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/ADV200004>
2. <https://www.autodesk.com/trust/security-advisories/adsk-sa-2020-0002>
3. https://chromereleases.googleblog.com/2020/04/stable-channel-update-for-desktop_15.html

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