**ממ״ן 12**

**שאלה 1:**

1. החולשה: קבלת השי חיובית בקרב אנשים שהקרדיט שלהם שלילי, למרות שנדרש מינימום קרדיט של 750 לשם קבלת השי.

זאת נעשה באמצעות ניצול לרעה של יכולת השוואה סמויה של מספרים מסומנים ולא מסומנים, שבה שני המספרים מיוחסים כלא מסומנים – ללא התראה ובאופן בלתי צפוי, בהכרח.  
נשים לב כי הקבוע uint bound = 750 הוא **uint** – שלם ללא סימן, בעוד credit הוא **int** – שלם עם סימן. שפת C++ נדרשת לבצע השוואה בין int לuint בערך ההחזרה – וכברירת מחדל היא תתייחס למידע בשני המספרים – כמספרים לא מסומנים.  
ההתקפה: אם לדוגמה, ליעל יש -1 שקלים בחשבון הבנק (או 0xFFFFFFFF ב32 סיביות), ולמעשה המחשב יתייחס לאותו ערך כ-4294967295 – בדיוק השלם הלא-מסומן שמיוצג ע״י הסיביות הנ״ל, ובוודאי שמתקיים כי 4294967295 > 750 – ועל כן הפונקציה תחזיר זכאות חיובית, למרות שבוודאי אם יש ליעל מינוס, היא לא זכאית!   
למעשה, זה יעבוד עבור כל קרדיט שלילי אפשרי – באופן זהה לחלוטין, בכל מחשב מודרני.

התיקון: פשוט מאוד. יש לשנות את ההגדרה בראש הפונקציה:

**unsigned** **int** bound = 750; -> **int** bound = 750;

הפתרון יגרום להשוואה להתבצע בין שני מספרים מסומנים, ובמקרה זה, גם אם יעל בעלת קרדיט שלילי בחשבון – **התשובה תהיה נכונה כי היחס לערכי המספרים יהיה נכון**.