תיאור חולשה

בקוד הנוכחי מתבצעת השוואה אשר בודקת האם משתנה מסוג int אשר מכיל ערך אפשרי בין 100- ל1000 גדול או שווה למשתנה מסוג unsigned int בעל הערך הקבוע 750.

כאשר מתבצעת השוואה בין 2 משתנים שאחד מהם הוא int והשני הוא unsigned int מתבצע casting למשתנה הint לunsigned int, בנוסף כאשר ממירים ערך int שלילי "קטן" לunsigned int מתקבל ערך חיובי מאוד גדול.

לכן, אם נצליח לגרום לערכו של המשתנה credit להיות שלילי, כאשר תתבצע השוואה הוא יעבור casting לunsigned int וכתוצאה מכך ערכו יהיה חיובי וגדול במיוחד כך שהתנאי יהיה נכון ויתקבל כי הלקוח זכאי לקבלת מתנה למרות שבפועל זה לא באמת נכון.

התקפה

בעקבות מה שתואר, אנו יודעים שעל מנת לנצל את החולשה ולהשיג מתנה ללקוח שאינו מגיעה לו מתנה, כל מה שעל יעל לעשות הוא להוריד את הקרדיט שלה למספר שלילי ובכך תנאי ההשוואה יהיה נכון ויעל תהיה זכאית למתנה.

תיקון

הערך המקסימלי של int הוא 2147483647 אשר בוודאי גדול מ750 ולכן אפשרי כי נשנה את סוג המשתנה bound מunsigned int לint והוא עדיין יכיל את הערך 750 ללא בעיה. ובנוסף בכך ש2 המשתנים יהיו מסוג int כאשר תתבצע השוואה, הערך של credit לא ישתנה ורק לקוחות אשר מגיעה להם מתנה יקבלו אותה.

```
bool is_entitled_for_promotional_gift(int ID)

{

        int bound = 750;

        int credit = get_credit(ID);

        return (credit >= bound);

}
```

רפרנסים

1. https://gcc.gnu.org/legacy-ml/gcc/2010-09/msg00504.html
הסבר על כך שהקומפיילר עושה casting מint ל unsigned int למשתנה כאשר יש השוואה בין 2 משתנים כאשר אחד מסוג int והשני מסוג unsigned int.

2. https://cwe.mitre.org/data/definitions/195.html
הסבר על כך שכאשר עושים casting לערך int שלילי קטן לunsigned int מתקבל ערך חיובי מאוד גדול.