פגיעות בפרוטוקול HTTP/2

עלולה לאפשר ביצוע מתקפות מניעת שירות

13/08/2025
י"ט אב תשפ"ה

[תקציר]

- CERT/CC פרסם פגיעות בפרוטוקול HTTP/2, שנמצאה על ידי חוקרי אונ' ת"א (גל בר-נחום, פרופ' ענת ברמלר-בר, ד"ר יניב הראל).
- הפגיעות עלולה לאפשר ביצוע מתקפות מניעת שירות רחבות היקף כנגד ציוד ותוכנות של יצרנים שונים.
- הפגיעות קיבלה את הכינוי "MadeYouReset" (CVE-2025-8671).

[פרטים]

- הפגיעות קיימת בשל שוני בין הגדרות הפרוטוקול לבין הארכיטקטורה הפנימית של שרתי Web שונים.
- ניצול הפגיעות עלולה ליצור מצב של חוסר משאבים (Resource Exhaustion) ומימוש מתקפת מניעת שירות.
- הפגיעות דווחה למספר רב של יצרנים (118). פירוט בקישור מס' 1.
- במועד הפרסום, 11 יצרנים מזוהים כפגיעים, 25 יצרנים מזוהים כלא פגיעים, והיתרה (82) מסווגים כלא-ידוע. לא כל היצרנים השיבו תשובה רשמית לפניית CERT/CC.
- פרטים נוספים על הפגיעות בקישור מס' 2.

פעולות מידיות לביצוע:

- מומלץ מאד לתעדף הטיפול בפגיעות זו, בפרט עבור מוצרים ותוכנות הנגישות ישירות מרשת האינטרנט.
- המשתמשים במוצרים ותוכנות שעבורם פורסם עדכון אבטחה לפגיעות זו על ידי היצרנים הרלוונטיים, מומלץ לבוחנם ולהתקינם בהקדם האפשרי (ראו קישור מס' 1).

⚠

שיתוף מידע עם מערך הסייבר 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.

[דרכי התמודדות]

- מומלץ מאד לתעדף הטיפול בפגיעות זו, בפרט עבור מוצרים ותוכנות הנגישות ישירות מרשת האינטרנט.
- משתמשים במוצרים ותוכנות שעבורם פורסם עדכון אבטחה לפגיעות זו על ידי היצרנים הרלוונטיים, מומלץ לבוחנם ולהתקינם בהקדם האפשרי (ראו קישור מס' 1).
- משתמשים במוצרים שעבורם טרם פורסם עדכון אבטחה לפגיעות זו, או שמצב פגיעותם עדיין אינו ידוע - מומלץ מאד לעקוב אחר פרסומי היצרנים הרלוונטיים בנדון, ואם יפורסם עדכון אבטחה לבוחנו ולהתקינו בהקדם האפשרי.
- כמעקף זמני בלבד, ניתן לבחון נטרול השימוש בפרוטוקול HTTP/2 עד לפרסום והתקנת העדכון במערכותיכם. על כל ארגון לשקול ולהחליט בנושא זה בהתאם לתפיסת הסיכון שלו מחד, וליתרונות של השימוש בפרוטוקול זה מאידך.
- אפשרות נוספת היא הגבלה על מספר/קצב הודעות מסוג RST_STREAMs הנשלחות מהשרת.

מקורות

1. https://www.kb.cert.org/vuls/id/767506
2. https://galbarnahum.com/made-you-reset