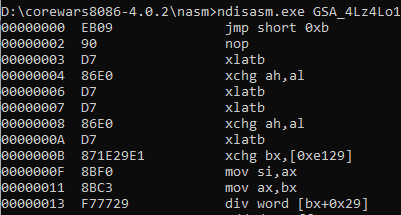
הנדסה לאחור ופריצה לבינארי של cgx 2022 survivors

עדכון שלי [איתי ברוק], עשיתי RE לקבוצה שהגיעה מקום 2 של phase1.  
שמתי לב לחולשה חמורה במימוש של כל אחד השורדים.

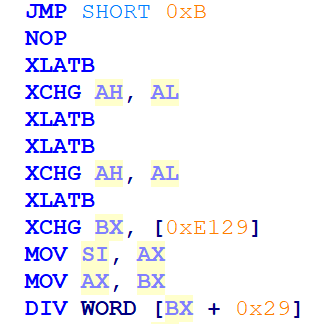
תיאור החולשה שגיליתי:  
נראה כי שורד 2 מעביר את **מיקומו** אל שורד 1 דרך **hardcoded** memory ceil  
על **הזירה**.  
יתרה מכך, שורד 1 לוקח את הערך במיקום הזה ובהמשך הקוד  
מוסיף לערך בתא היסט hardcoded ומחלק בערך שנמצא בתא שקיבל!

ניצול:  
ראשית ניצול לשיבוש שורד 1:  
הכנסה של ערך מתאים 0 אל התא המתאים [surviver2 start position + 0x29] כדי ששורד 1 יגיע למצב של segmentation fault על חלוקה באפס.

קטע הקוד הפגיע [לאוהבי השחור לבן של terminal]:



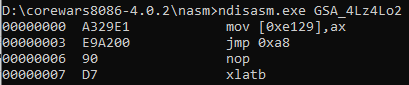
קטע הקוד הפגיע [לאוהבי הלבן צבעוני שלnotepad++ ]:



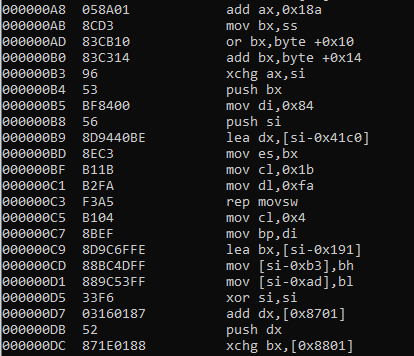
ניצול החולשה שיבוש אל שורד 2:

נשים לב שנוכל לקחת אלינו את הערך של המיקום ההתחלתי שלו שהוא שם בתא בזכרון ומשם הוא מבצע קפיצה בלתי מותנית ואז פעולות בצורה סדרתית.  
נקדים לחשב את המיקום שהוא יגיע אליו ונוכל להזריק אליו פקודה לא חוקית כדי שיעוף עליה או אף להשתמש בו והקפיץ אותו אל trap שתשמש לטובתנו

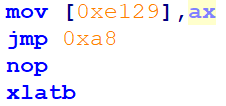
קטע הקוד הפגיע [לאוהבי השחור לבן של terminal]:



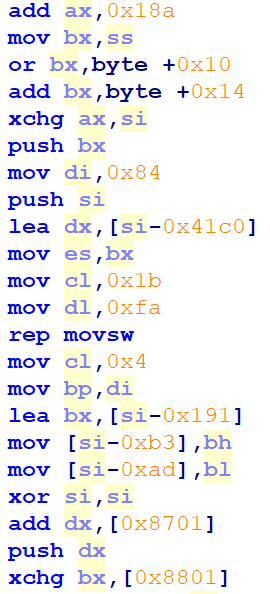
; some more code here



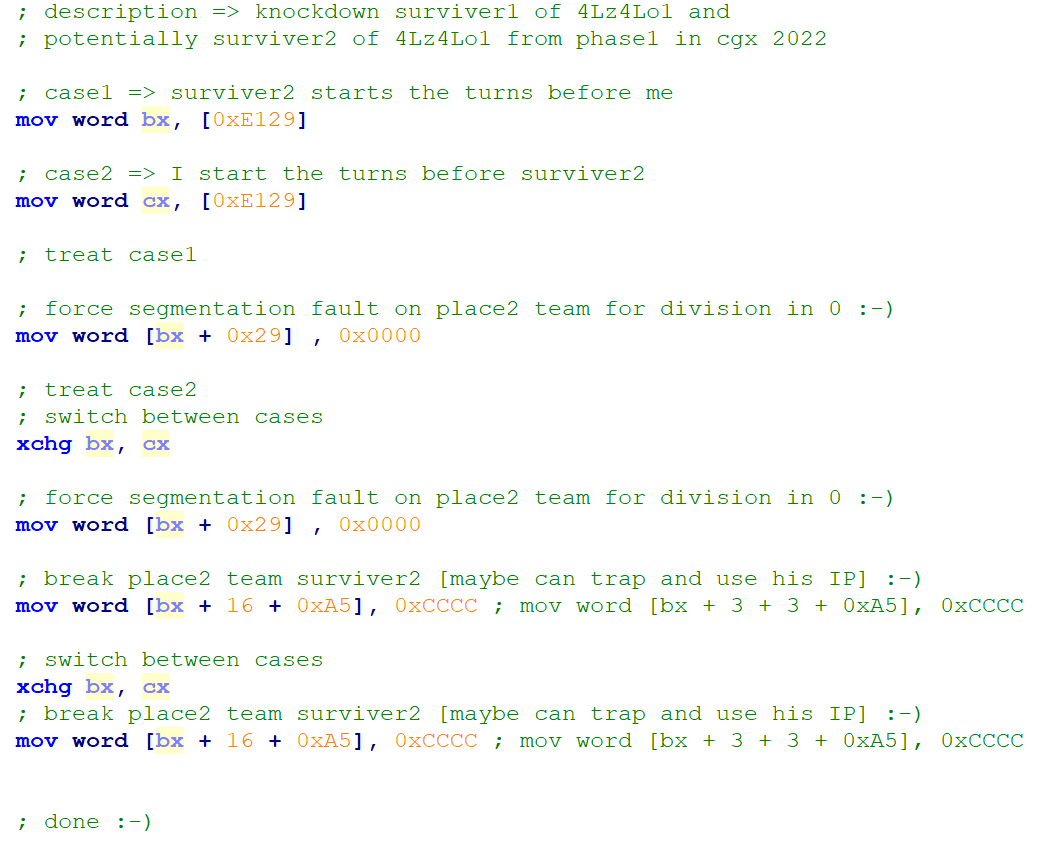
קטע הקוד הפגיע [לאוהבי הלבן צבעוני שלnotepad++ ]:



; some more code here



השמשה:



נחשב את האפשרויות שבהן עובדת ההתקפה:

עלול להשתנות לפי סדר ביצוע הפקודה בהרצה על ידי המנוע.

סימונים וקיצורים:

ממיונים לפי סדר ביצוע פקודה בתור משמאל המוקדם ביותר ימינה

L1, L2 קיצור לקבוצה 4Lz4Lo שורד 1 ושורד 2 בהתאמה

D1 גם לקבוצה שלנו DirtyBAU

GOOD הכוונה חוסלו BAD הכוונה שרדו את ההתקפה

FORMAT := permutation from {L1, D2, L2}: value from {GOOD, BAD}

L1 D2 L2: BAD

L1 L2 D2: GOOD

L2 D2 L1: GOOD

L2 L1 D2: GOOD

D2 L1 L2: GOOD

D2 L2 L1: GOOD

בדיקה לאחר השמשה:



סיכום:

בכל אחד מהם חולשה חביבה השנייה במיוחד ובהן וקטור תקיפה פשוט למדי ואפקטיבי.