15 נובמבר 2020
כ"ח חשון תשפ"א
סימוכין:ב-ס-1202

חזרתה של מתקפת DNS Cache Poisoning

תקציר

לאחרונה פורסם מחקר אשר עלול לחדש את האפשרות לביצוע תקיפות מסוג Cache Poisoning כנגד שרתי DNS.
מסמך זה יסקור את התקיפה ודרכים להתמודדות עימה.

פרטים

1. בשנת 2008 פרסם החוקר דן קמינסקי מידע לגבי האפשרות לבצע תקיפות מסוג DNS Cache poisoning.
2. התקיפה מאפשרת לתוקף להזין כתובות IP של שרתים בשליטתו לשרתי DNS המבצעים Caching לשיפור הביצועים, וכך לגרום להסטת התעבורה אל שרתים אלו.
3. מימוש התקיפה עלול לאפשר תקיפות התחזות (Spoofing) או יירוט תעבורה מסוג MITM (Man In The Middle).
4. התקיפות התבססו על כך ששדה Transaction ID בשאילתת DNS יכול להכיל רק 65K ערכים.
5. בתגובה למתקפה זו, החלו שרתי DNS לבצע שאילתות DNS באמצעות פורטים אקראיים, כך שכעת התוקף נאלץ למצוא גם את ה- Transaction ID וגם את פורט המקור של התעבורה, דבר שהפך את המתקפה לבלתי מעשית.
6. לאחרונה גילו חוקרים כי ניתן לזהות את פורטי המקור של תעבורת ה-DNS באמצעות Side Channel Attack המתבססת על פניות מהירות לכ-

1000 פורטים בשניה, וניתוח תעבורת ה-ICMP הנגרמת כתוצאה מפניות אלו.

7. אם המתקפה מצליחה ופורט המקור מזוהה, ניתן לבצע את מתקפת ה-DNS Cache Poisoning הקלסית מ-2008.
8. מקור הפגיעות בשימוש בערך קבוע וידוע עבור ה- ICMP Global Rate Limit.
9. הפגיעות קיבלה את הזיהוי CVE-2020-25705 ואת הכינוי SAD DNS.
10. מערכות ההפעלה הפגיעות כוללות גרסאות שונות של מערכות ההפעלה Windows, MacOS, Linux, FreeBSD:

- Linux 3.18-5.10
- Windows Server 2019 (version 1809) and newer
- macOS 10.15 and newer
- FreeBSD 12.1.0 and newer

עבור מערכות ההפעלה **שאינן לינוקס**, לא נבדקו גרסאות ישנות יותר, וייתכן שגם הן פגיעות.

11. המחקר דיווח כי מבחינה שערכו החוקרים, עולה כי כ-34% מהשרתים הרלוונטיים באינטרנט, פגיעים.

דרכי התמודדות

1. עבור מערכות הפעלה שהוצא עבורן עדכון למתקפה זו, מומלץ לבחון ולהתקין בהקדם האפשרי את עדכון האבטחה. העדכון מבוסס על ערך אקראי ל-ICMP Global Rate Limit.
2. אם עדיין לא הוצא עדכון למערכת ההפעלה שבשימושכם, ניתן זמנית לנטרל את המתקפה עד להתקנת עדכון באמצעות חסימת תעבורת ICMP יוצאת משרת ה-DNS. מומלץ לבחון נטרול הודעות ICMP Port Unreachable יוצאות בלבד, ולא את כל פרוטוקול ICMP.
3. אם ניתן להפעיל אחד מהשירותים שנועדו לאבטחת DNS, כגון DNSSEC או DNS Cookie, הם יכולים לסייע במניעת המתקפה.

4. הקטנת ערך ה-Timeout לשאילתות של שרת ה-DNS עשויה לסייע במניעת המתקפה, אך עלולה להגדיל את התעבורה והעומס על השרת.

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

מקורות

1. https://www.cs.ucr.edu/~zhiyunq/SADDNS.html
2. https://blog.cloudflare.com/sad-dns-explained/
3. https://www.zdnet.com/article/dns-cache-poisoning-poised-for-a-comeback-sad-dns/
4. https://thehackernews.com/2020/11/sad-dns-new-flaws-re-enable-dns-cache.html
5. https://www.bleepingcomputer.com/news/security/dns-cache-poisoning-attacks-return-due-to-linux-weakness/
6. https://www.blackhat.com/presentations/bh-jp-08/bh-jp-08-Kaminsky/BlackHat-Japan-08-Kaminsky-DNS08-BlackOps.pdf

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