30 יולי 2019
כ"ז תמוז תשע"ט
[עדכון]:08 ספטמבר 2019
ח' אלול תשע"ט
[עדכון2]:03 נובמבר 2019
ה' חשון תש"פ
סימוכין:ב-ס-979B

[עדכון2] BlueKeep - פגיעות קריטית בשירות Remote Desktop Services בגרסאות ישנות של מערכת ההפעלה Windows

תקציר

מיקרוסופט פרסמה בחודש מאי האחרון כי זוהתה פגיעות קריטית בשירות Remote Desktop Services (CVE-2019-0708), המשמש לגישה מרחוק לתחנות עבודה ושרתים הפועלים על גבי מערכת ההפעלה Windows, בגרסאות ישנות.

הגרסאות הפגיעות הינן Windows XP, 2003, 7, 2008.

מערך הסייבר הלאומי התריע מיד לאחר הפרסום לגבי הצורך לעדכן מערכות הפעלה אלו.

[עדכון 2] בימים האחרונים זוהתה פעילות תקיפה המנצלת פגיעות זו להתקנת פוגען המבצע כריית מטבעות וירטואליים.

אנו חוזרים וממליצים בתוקף לבחון ולהתקין את עדכוני האבטחה הרלוונטיים בהקדם האפשרי.

פרטים

1. הפגיעות עלולה לאפשר לתוקף לא מזוהה הרצת קוד מרחוק והשתלטות על המחשב המותקף.

2. הפגיעות מאפשרת יצירת פוגען מסוג תולעת (Worm), העובר באופן עצמאי בין מחשבים החשופים לפגיעות זו, באופן דומה לתולעת WannaCry שפעלה לפני כשנתיים תוך ניצול פגיעות בפרוטוקול שונה.
3. עקב אפשרות זו לפגיעה רחבה, מיקרוסופט הוציאה עדכוני אבטחה לפגיעות זו אף למערכות הפעלה מיושנות (XP, 2003) שאינן נתמכות באופן סדיר.
4. מבין מערכות ההפעלה הנתמכות על ידי החברה, הפגיעות קיימת בגרסאות:

- Windows 7 for 32-bit Systems Service Pack 1
- Windows 7 for x64-based Systems Service Pack 1
- Windows Server 2008 for 32-bit Systems Service Pack 2
- Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)
- Windows Server 2008 for Itanium-Based Systems Service Pack 2
- Windows Server 2008 for x64-based Systems Service Pack 2
- Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)
- Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1
- Windows Server 2008 R2 for x64-based Systems Service Pack 1
- Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)

5. בשל פוטנציאל הנזק הגבוה, החברה פרסמה עדכון אבטחה גם לגרסאות הבאות של מערכות הפעלה שכבר אינן נתמכות:

- Windows XP SP3 x86
- Windows XP Professional x64 Edition SP2
- Windows XP Embedded SP3 x86
- Windows Server 2003 SP2 x86
- Windows Server 2003 x64 Edition SP2

6. לאחרונה פורסמו מצגות המתארות במדויק את השלבים הנדרשים למימוש הפגיעות לשם הרצת קוד מרחוק על המחשב המותקף.

7. בנוסף, זוהה ברשת וריאנט של פוגען בשם **Watchbog**, המשמש לכריית מטבעות וירטואליים, אשר בין השאר סורק אחר מחשבים החשופים לפגיעות זו, ככל הנראה על מנת לנצלם בתקיפה עתידית.
8. חברה בשם **Immunity**, המוכרת למנוייה תוכנה המשמשת למבדקי חוסן של מערכות מחשוב, פרסמה עדכון המאפשר לממש הפגיעות באמצעות התוכנה.
9. [עדכון] פורסם פומבית **Exploit** המאפשר לממש את הפגיעות להרצת קוד מרחוק.
10. אוסף האירועים הללו מגדיל מאד את הסיכון לתקיפה קרובה כנגד מחשבים אשר טרם הותקן בהם העדכון.
11. [עדכון 2] זוהתה פעילות תקיפה המנצלת פגיעות זו להתקנת פוגען לכריית מטבעות וירטואליים מסוג **Monero**.

דרכי התמודדות

1. למשתמשים ארגוניים, מומלץ לבחון העדכונים במערכות ניסוי, ולעדכן מערכות הייצור בהקדם האפשרי.
2. למשתמשים פרטיים במערכות נתמכות, מומלץ להתקין העדכון בהקדם באמצעות המנגנונים המובנים לעדכון מערכת ההפעלה.
3. למשתמשים במערכות שאינן נתמכות, יש להתקין העדכונים מהקישור הבא:

https://support.microsoft.com/en-us/help/4500705/customer-guidance-for-cve-2019-0708

בנוסף, מומלץ לבחון בהקדם האפשרות לשדרוג מערכת ההפעלה לגרסה עדכנית ונתמכת.

4. מומלץ לא לחשוף ממשקי **Remote Desktop Services** לרשת האינטרנט. מומלץ לוודא כי פורט **TCP/3389** (פורט ברירת המחדל לשירות זה), או כל פורט אחר בו בחרתם להפעיל שירות זה, אינו נגיש למערכותיכם מרשת האינטרנט. אם משיקולים עסקיים נדרשת נגישות מסוג זה

מרשת האינטרנט, מומלץ ליישמה תוך שימוש ב- VPN עם הצפנה והזדהות מתאימים.

5. כמעקף זמני וחלקי בלבד, ניתן לוודא כי מופעל בעמדה מנגנון Network Level Authentication (NLA). המנגנון מחייב ביצוע הזדהות על ידי התוקף טרם ניצול הפגיעות. המעקף הינו חלקי בלבד כי אם ברשות התוקף נתוני ההזדהות, בין אם השיגם מראש ובין אם על ידי ניחוש סיסמאות וכד', התקיפה עדיין עלולה להתממש. לכן, מומלץ להתקין העדכונים בהקדם גם אם NLA מופעל בעמדה.
6. אם אינכם עושים שימוש בשירות Remote Desktop Services, מומלץ לנטרלו.

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

מקורות

1. https://blogs.technet.microsoft.com/msrc/2019/05/14/prevent-a-worm-by-updating-remote-desktop-services-cve-2019-0708/
2. https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0708
3. https://support.microsoft.com/en-us/help/4500705/customer-guidance-for-cve-2019-0708
4. https://support.microsoft.com/en-us/help/4500331/windows-update-kb4500331
5. https://securingtomorrow.mcafee.com/other-blogs/mcafee-labs/rdp-stands-for-really-do-patch-understanding-the-wormable-rdp-vulnerability-cve-2019-0708/
6. https://www.gov.il/he/departments/publications/reports/rdp-critical
7. https://www.gov.il/he/departments/publications/reports/rdp-critical-update
8. https://doublepulsar.com/bluekeep-exploitation-activity-seen-in-the-wild-bd6ee6e599a6
9. https://www.kryptoslogic.com/blog/2019/11/bluekeep-cve-2019-0708-exploitation-spotted-in-the-wild/

שיתוף מידע עם הCERT הלאומי איננו מחליף חובת דיווח לגוף מנחה כלשהו, במידה שהתגלה צורך כזה