14 ינואר 2020
י"ז טבת תש"פ
סימוכין:ב-ס-1020

התרעה דחופה: פגיעות במערכות ההפעלה Windows10, Windows Server 2016,2019,Server Core

תקציר

1. בעדכון האבטחה החודשי של חברת מיקרוסופט, שהתפרסם היום, 14/1/2020, פורסמה פגיעות הניתנת לניצול על ידי תוקף, להטעיית המשתמש ומערכת ההפעלה באמצעות תעודה דיגיטלית מזויפת.
2. מומלץ מאד להתקין את עדכון האבטחה הרלוונטי, בכל המחשבים בארגונכם, ולתעדף את סדר העדכונים על פי המפורט בסעיף "דרכי התמודדות" להלן.

פרטים

1. הפגיעות קיימת בגרסאות מערכת ההפעלה Windows10, Windows Server 2016, 2019, Server Core.
2. מקור הפגיעויות ברכיב הקריפטוגרפי crypt32.dll, המשמש לטיפול, בדיקה ואישור של תעודות דיגיטליות ומסרים קריפטוגרפיים. הפגיעות מאפשרת הטעיה של מערכת ההפעלה והמשתמש בנוגע לאותנטיות של תעודה דיגיטלית או מסר קריפטוגרפי המוצג להם.
3. הפגיעות ניתנת לניצול באמצעות זיוף חתימה דיגיטלית על קבצים, לדוגמה, חתימה על קובץ ריצה עוין באמצעות חתימה הנחזית כזו של חברת מיקרוסופט. יצוין כי לעיתים מערכות אבטחה מוגדרות כך שזיהוי קבצים כחתומים על ידי מיקרוסופט, גורם לבדיקה פחות מחמירה של הקבצים או לדילוג על הבדיקה כלל.

4. בנוסף, הפגיעות ניתנת לניצול באמצעות התחזות לשרת בתקיפה מסוג Man In The Middle (MITM).
5. **מניסיון העבר, פגיעות זו עלולה להפוך במהירות לתקיפה פעילה, מאחר ופוטנציאל התקיפה הוא חריג בגודלו.**
6. **כל מחשב המריץ גרסה פגיעה של מערכת ההפעלה, עלול להיות יעד לתקיפה.**

דרכי התמודדות

1. משתמשים פרטיים, מומלץ **מיידית** לבצע **עדכון יזום** ("Update Now") של מערכת ההפעלה באמצעות הכלים המובנים בה.
2. משתמשים ארגוניים - **מומלץ מאד להתקין את עדכון האבטחה של החברה, לאחר בדיקות מזורזות כי אין מניעה לכך, בכל המחשבים בארגונכם**, ולתעדף את התקנת העדכונים על פי הסדר הבא:
   1. כל שרת ותחנה המוודאים באופן שוטף חתימות TLS/SSL או תעודות דיגיטליות כחלק מפעולתם. לדוגמה - שרתי Web, שרתי Proxy, שרתי Exchange וכד'.
   2. שרתים ועמדות קצה המשמשים לתהליכים קריטיים בארגון, או שגורמים רבים בארגון מסתמכים על פעולה תקינה שלהם. דוגמה - Domain Controllers, שרתי DNS ארגוניים, שרתי VPN, שרתי עדכוני תוכנה, שרתי SharePoint וכו'.
   3. עמדות קצה החשופות לרשת האינטרנט או משמשות באופן שוטף מנהלנים בעלי הרשאות גבוהות לניהול הרשת.
   4. עמדות קצה של משתמשים רגילים העושים שימוש בתוכנת Office, בתוכנות מבוססות NET. וכד'.
3. יודגש כי יש להכין תוכנית עדכון הכוללת **את כלל העמדות המפעילות מערכות הפעלה מתוצרת החברה בארגון**, הן ברשת הארגונית, הן ב-DMZ והן ברשת הנגישה לאינטרנט.

מקורות

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0601

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