* 1. ליקויים בהגדרות ה-Group Policy.

פירוט הממצא:

במהלך הבדיקה נמצא כי קיימים מספר ליקויים בהגדרות ה-Group Policy:

1. ההגדרה Password History Count אינה מוגדרת כראוי.
2. ההגדרה Maximum password Age אינה מוגדרת כראוי.
3. ההגדרה Minimum Password Age אינה מוגדרת כראוי.
4. ההגדרה Minimum password Length אינה מוגדרת כראוי.
5. ההגדרה Enable password Complexity אינה מוגדרת כראוי.
6. ההגדרה Disable reverse encryption to passwords אינה מוגדרת כראוי.
7. ההגדרות Account lockout duration ו-Account lockout threshold אינן מוגדרות כראוי.
8. ההגדרה account lockout counter אינה מוגדרת כראוי.

סבירות מימוש הנזק: בינונית

חומרת הנזק: בינונית

רמת הסיכון: בינונית

פירוט הסיכון:

1. הגדרת מדיניות זו קובעת את מספר הסיסמאות המחודשות והייחודיות שיש לשייך לחשבון משתמש לפני שיהיה אפשר לעשות שימוש חוזר בסיסמה ישנה. הערך עבור הגדרת מדיניות זו חייב להיות בין 0 ל-24 סיסמאות. ערך ברירת המחדל הוא 0 סיסמאות, אך הגדרת ברירת המחדל בתחום היא 24 סיסמאות. כדי לשמור על האפקטיביות של הגדרת מדיניות זו, השתמש בהגדרת גיל הסיסמה המינימלי כדי למנוע ממשתמשים לשנות שוב ושוב את הסיסמה שלהם.
2. ההגדרה Maximum password age מגדירה כמה זמן משתמש יכול להשתמש בסיסמה לפני שתוקפה פג. הערכים עבור הגדרת מדיניות זו נעים בין 0 ל-999 ימים. אם הערך מוגדר ל-0 הסיסמה הסיסמה לעולם לא תפוג. מכיוון שתוקפים יכולים לפצח סיסמאות, ככל שתשונה הסיסמה בתדירות גבוהה יותר פחות הזדמנות שתוקף יוכל להשתמש בסיסמאות ישנות.
3. במצב בו מדיניות מספר הימים המינימאלי לשינוי הסיסמאות הינה מיידית, שילוב שינויי סיסמה מיידיים עם היסטוריית זכירת הסיסמאות מאפשר למשתמש לשנות סיסמה שוב ושוב עד למילוי דרישת היסטוריית הסיסמה ולשימוש חוזר בסיסמה המקורית. לדוגמה, נניח שהסיסמה היא "Aa@12345" והדרישה להיסטוריה היא 24. אם גיל הסיסמה המינימאלי הוא 0, ניתן לשנות את הסיסמה 24 פעמים ברציפות עד שלבסוף הסיסמה תחזור ל-"Aa@12345".
4. העדר מדיניות סיסמאות מוקשחת לשרת המערכת עלול להוביל למצב בו מתבצע שימוש בסיסמה פשוטה ויחסית קלה לניחוש, מה שמסייע רבות לתוקף לבצע מתקפות מילון ו-Brute Force, מתקפות אלו עשויות להתבצע בקלות יתרה עקב העדר הגדרת ה-Account Lockout. לאחר ביצוע מתקפות אלו, תוקף עלול להשיג גישה לשרת בהרשאות גבוהות, ולבצע הקרסה של השרת ואף הצפנת הנתונים שלו.
5. ההגדרה Password complexity מוודאה כי כלל הסיסמאות החדשות עומדות בדרישות בסיסיות ליצירת סיסמה חזקה.  
   כאשר הגדרה זו מופעלת, על הסיסמאות לעמוד בדרישות הבאות:

* אורך הסיסמה מינימום 8 תווים.
* מכילים 3 תווים מהקטגוריות הבאות:

אותיות גדולות, אותיות קטנות, ספרות ותווים מיוחדים.

1. ההגדרה Disable reverse encryption to passwords קובעת האם מערכת ההפעלה שומרת סיסמאות באופן המאפשר שימוש בהצפנה הפיכה, המספקת תמיכה בפרוטוקולי יישומים הדורשים מידע על סיסמת המשתמש למטרות אימות. סיסמאות המאוחסנות עם הצפנה הפיכה זהות למעשה לסיסמאות המשתמשים הנשמרות כ-Clear text.
2. העדר נעילת המשתמשים ברשת הארגונית אחרי כמות ניסיונות התחברות כושלים עלול להוביל למצב בו כל משתמש ברשת הארגון בעל גישה תקשורתית אל השרת יוכל לנסות להזדהות אל השרת ללא הגבלה עקב העדר מנגנון נעילה. הגדרה זו מעלה משמעותית את הסיכוי שתוקף יצליח לקבל גישה אל השרת באמצעות מתקפת Brute Force או מתקפות מילון.
3. משתמשים עלולים לנעול עצמם מחוץ למחשב במידה והם מזינים את הסיסמה שלהם בצורה שגויה מספר פעמים. על מנת להפחית את הסיכון לנעילות שכאלה, ההגדרה קובעת את מספר הדקות שעוברות לפני שהמונה שסופר את הניסיונות הכושלים מתאפס.

המלצות לתיקון:

* מומלץ להגדיר את ה- Password History Countל-24 סיסמאות או פחות, אך לא ל-0 בנתיב הבא:  
  Computer Configuration\Policies\Windows Settings\Security Settings\Account Policies\Password Policy\Password History Count
* מומלץ להגדיר את ה- Maximum password ageל-60 ימים או פחות, אך לא ל-0 בנתיב הבא:  
  Computer Configuration\Policies\Windows Settings\Security Settings\Account Policies\Password Policy\Maximum password age
* מומלץ להגדיר את ה-Minimum password age ליום אחד או יותר בנתיב הבא:  
  Computer Configuration\Policies\Windows Settings\Security Settings\Account Policies\Password Policy\Minimum password age
* מומלץ להגדיר את ההגדרה Minimum password length ל-14 תווים או יותר בנתיב הבא:  
  Computer Configuration\Policies\Windows Settings\Security Settings\Account Policies\Password Policy\Minimum password length
* מומלץ להגדיר את ההגדרה Password Complexity ל-Enabled בנתיב הבא:  
  Computer Configuration\Policies\Windows Settings\Security Settings\Account Policies\Password Policy\Password must meet complexity requirements
* מומלץ להגדיר את ההגדרה Disable reverse encryption to password ל-Enabled בנתיב הבא:  
  Computer Configuration\Policies\Windows Settings\Security Settings\Account Policies\Password Policy\Store passwords using reversible encryption
* מומלץ להגדיר את ההגדרה Account lockout duration ל-15 דקות או יותר בנתיב הבא:  
  Computer Configuration\Policies\Windows Settings\Security Settings\Account Policies\Account Lockout Policy\Account lockout duration
* מומלץ להגדיר את ההגדרה Account lockout threshold בין 0 ל-10 ניסיונות התחברות כושלים בנתיב הבא:  
  Computer Configuration\Policies\Windows Settings\Security Settings\Account Policies\Account Lockout Policy\Account lockout threshold
* מומלץ להגדיר את ההגדרה account lockout counter לכ-15 דקות או יותר בנתיב הבא:  
  Computer Configuration\Policies\Windows Settings\Security Settings\Account Policies\Account Lockout Policy\Account lockout duration
  1. ליקויים בהגדרת הרשאות משתמשים.

פירוט הממצא:

במהלך הבדיקה נמצא כי קיימים מספר ליקויים בהגדרת הרשאות המשתמשים בשרת המערכת:

1. ההגדרה Access Credential Manager as a trusted caller אינה מוגדרת כראוי.
2. ההגדרה Act as part of the operating system אינה מוגדרת כראוי.
3. ההגדרה Adjust memory quotes for a process אינה מוגדרת כראוי.
4. ההגדרה Back up files and directories אינה מוגדרת כראוי.
5. ההגדרה change the system time אינה מוגדרת כראוי.
6. ההגדרה change the time zone אינה מוגדרת כראוי.
7. ההגדרה create a pagefile אינה מוגדרת כראוי.
8. ההגדרה Add workstations to domain אינה מוגדרת כראוי.
9. ההגדרה Create a token object אינה מוגדרת כראוי.
10. ההגדרה Create global object אינה מוגדרת כראוי.
11. ההגדרה Create permanent shared objects אינה מוגדרת כראוי.
12. ההגדרה Debug programs אינה מוגדרת כראוי.
13. ההגדרה Deny log on as a batch job אינה מוגדרת כראוי.
14. ההגדרה Deny log on as a service אינה מוגדרת כראוי.
15. ההגדרה Deny log on locally אינה מוגדרת כראוי.
16. ההגדרה Deny log on through Remote Desktop Services אינה מוגדרת כראוי.
17. ההגדרה Force shutdown from a remote system אינה מוגדרת כראוי.
18. ההגדרה Generate security audits אינה מוגדרת כראוי.
19. ההגדרה Increase scheduling priority אינה מוגדרת כראוי.
20. ההגדרה Load and unload device drivers אינה מוגדרת כראוי.
21. ההגדרה Lock pages in memory אינה מוגדרת כראוי.
22. ההגדרה Log on as a batch job אינה מוגדרת כראוי.
23. ההגדרה Modify an object label אינה מוגדרת כראוי.
24. ההגדרה Modify firmware environment values אינה מוגדרת כראוי.
25. ההגדרה Perform volume maintenance tasks אינה מוגדרת כראוי.
26. ההגדרה Profile single process אינה מוגדרת כראוי.
27. ההגדרה Profile system performance אינה מוגדרת כראוי.
28. ההגדרה Replace a process level token אינה מוגדרת כראוי.
29. ההגדרה Restore files and directories אינה מוגדרת כראוי.
30. ההגדרה shut down the system אינה מוגדרת כראוי.
31. ההגדרה Synchronize directory service data אינה מוגדרת כראוי.
32. ההגדרה Take ownership of files or other objects אינה מוגדרת כראוי.

סבירות מימוש הנזק: בינונית

חומרת הנזק: בינונית

רמת הסיכון: בינונית

פירוט הסיכון:

1. ההגדרה Access Credential Manager as a trusted caller משמשת את מנהל האישורים במהלך הגיבוי והשחזור. לאף חשבון לא צריכה להיות זכות משתמש זו, מכיוון שהיא מוקצית רק ל-Winlogon. פרטי הכניסה השמורים של המשתמשים עלולים להיפגע אם זכות משתמש זו מוקצית לגופים אחרים.
2. ההגדרה Act as part of the operating system לתהליך לקבל את זהותו של כל משתמש וכך לקבל גישה למשאבים שהמשתמש מורשה לגשת אליהם. המשתמשים בעליי הרשאה זו יכולים להשתלט על המחשב ולמחוק עדויות לכל פעילויות שבוצעו על המחשב.
3. ההגדרה Adjust memory quotes for a process מאפשרת למשתמש להתאים את כמות הזיכרון המרבית הזמינה לתהליך. היכולת להתאים מכסות זיכרון שימושית לכוונון המערכת, אך ניתן לנצל אותה לרעה. בידיים הלא נכונות, זה יכול לשמש להפעלת מתקפת מניעת שירות (DoS).
4. ההגדרה Back up files and directories מאפשרת למשתמשים לעקוף הרשאות קבצים וספריות לגיבוי המערכת. הרשאה של המשתמש מופעלת רק כאשר יישום (כגון NTBACKUP) מנסה לגשת לקובץ או לספרייה דרך ממשק תכנות היישומים לגיבוי מערכת הקבצים NTFS (API). אחרת, הרשאות הקבצים והספריות שהוקצו חלות.
5. ההגדרה change the system time קובעת אילו משתמשים וקבוצות יכולים לשנות את השעה והתאריך בשעון הפנימי של המחשבים בסביבתכם. משתמשים שמוקצים להם זכות משתמש זו יכולים להשפיע על הופעת יומני האירועים. כאשר הגדרת השעה של המחשב משתנה, תיעוד האירועים משקפים את הזמן החדש, ולא את הזמן בו התרחשו האירועים.
6. ההגדרה change the time zone קובעת אילו משתמשים יכולים לשנות את אזור הזמן של המחשב. יכולת זו אינה טומנת בחובה סכנה גדולה עבור המחשב ועשויה להיות שימושית עבור עובדים ניידים.
7. ההגדרה create a pagefile מאפשרת למשתמשים לשנות את גודל ה-pagefile. על ידי הפיכת ה-pagefile לגדול או קטן במיוחד, תוקף יכול להשפיע בקלות על ביצועיו של מחשב שנפגע.
8. ההגדרה Add workstations to domain מציינת אילו משתמשים יכולים להוסיף תחנות עבודה ל-Domain. משתמשים עם הרשאה זו יכולה להוסיף מחשב ל-Domain שמוגדר בצורה שמפרה מדיניות אבטחה ארגונית.
9. ההגדרה Create a token object לתהליך ליצור Token גישה, שעשוי לספק הרשאות גישה לנתונים רגישים. לחשבון משתמש שניתנת לו זכות משתמש זו יש שליטה מלאה על המערכת ויכולה להוביל לפגיעה במערכת. מומלץ מאוד שלא להקצות משתמש בעל הרשאה זו.
10. ההגדרה create global object קובעת אם משתמשים יכולים ליצור אובייקטים גלובליים הזמינים לכל ההפעלות. משתמשים עדיין יכולים ליצור אובייקטים ספציפיים להפעלה שלהם אם אין להם הרשאות משתמש זה.  
    משתמשים שיכולים ליצור אובייקטים גלובליים עשויים להשפיע על תהליכים שרצים תחת הפעלות של משתמשים אחרים. יכולת זו עלולה להוביל למגוון בעיות, כגון כשל ביישומים או השחתת נתונים.
11. ההגדרה Create permanent shared objects מאפשרת ליצור שיתוף של אובייקטים קבועים. משתמשים שיש להם הרשאה ליצור שיתוף של אובייקטים משותפים קבועים יכולים ליצור שיתוף חדש וע"י כך לחשוף נתונים רגישים לרשת.
12. ההגדרה Debug programs קובעת אילו חשבונות משתמשים יהיו בעלי הרשאה לצרף באגים לתהליך כלשהו או לליבה, המספקת גישה מלאה לרכיבי מערכת הפעלה רגישים וקריטיים. למפתחים שמנקים באגים ביישומים שלהם אין צורך להקצות זכות משתמש זו. עם זאת, מפתחים שמנקים באגים ברכיבי מערכת חדשים יזדקקו לכך.
13. ההגדרה Deny log on as a batch job קובעת אילו חשבונות לא יוכלו להיכנס למחשב כ-batch job. חשבונות המשתמשים במתזמן המשימות לתזמון עבודות זקוקים להרשאה זו. הרשאה זו יכולה לשמש לחשבונות לתזמן פעולות שצורכות משאבי מערכת מוגזמים, דבר העלול להוביל ל-DoS.
14. ההגדרה Deny log on as a service קובעת אילו חשבונות מנועים מלהתחבר כ-Services. באמצעות חשבונות שיכולים להיכנס כ Service ניתן להגדיר ולהתחיל שירותים לא מורשים, כגון מפתחות או תוכנות זדוניות אחרות.
15. ההגדרה Deny log on locally קובעת אילו משתמשים מונעים להתחבר למחשב באופן מקומי. אם הרשאת משתמש זו אינה מוגבלת, משתמשים לא מורשים עשויים להוריד ולהריץ תוכנות זדוניות.
16. ההגדרה Deny log on through Remote Desktop Services קובעת אילו משתמשים לא יכולים להתחבר למחשב מרחוק (באמצעות Remote Desktop). משתמשים לא מורשים עשויים להוריד ולהפעיל תוכנות זדוניות שמעלות את ההרשאות שלהן.
17. ההגדרה Force shutdown from a remote system מאפשרת למשתמשים לכבות מחשבים ממיקומים מרוחקים ברשת. כל מי שהוקצה לו זכות משתמש זו יכול לגרום למצב של מניעת שירות (DoS), מה שהופך את המחשב ללא זמין לבקשות המשתמש בשירות. לכן, מומלץ להקצות רק למנהלי מערכת מהימנים זכות משתמש זו.
18. ההגדרה Generate security audits קובעת אילו משתמשים או תהליכים יכולים ליצור רשומות ביקורת ביומן האבטחה.
19. ההגדרה Increase scheduling priority קובעת אם משתמשים יכולים להגדיל את העדיפות הבסיסית של תהליך. (אין זו פעולה מועדפת להגדיל את העדיפות היחסית בכיתת עדיפות.) זכות משתמש זו אינה נדרשת על ידי כלים ניהוליים המסופקים עם מערכת ההפעלה, אך ייתכן שהיא נדרשת על ידי כלי פיתוח תוכנה.
20. ההגדרה Load and unload device drivers מאפשרת למשתמשים לטעון באופן דינמי מנהל התקן חדש במערכת. תוקף יכול להשתמש ביכולת זו כדי להתקין קוד זדוני שנראה כמנהל התקן. הרשאת משתמש זו נדרשת למשתמשים להוסיף מדפסות מקומיות או מנהלי התקן למדפסת.
21. ההגדרה Lock pages in memory מאפשרת לתהליך לשמור נתונים בזיכרון הפיזי, מה שמונע מהמערכת את ההעברה של הנתונים לזיכרון הווירטואלי בדיסק. אם הרשאה זו מוקצית, יכולה להיות השפעה משמעותית על ביצועי המערכת. משתמשים עם הרשאת משתמש זו בזיכרון יכולים להקצות זיכרון פיזי למספר תהליכים, שעלולים להשאיר מעט RAM או ללא זיכרון RAM לתהליכים אחרים ולהביא למצב של DoS.
22. ההגדרה Log on as a batch job מאפשרת לחשבונות להתחבר באמצעות שירות מתזמן המשימות. השימוש בה צריך להיות מוגבל בסביבות אבטחה גבוהות למנוע שימוש לרעה במשאבי המערכת או למנוע מהתוקפים להשתמש בהרשאה זו להזרקת קוד זדוני לאחר קבלת גישה ברמת המשתמש למחשב.
23. ההגדרה Modify an object label קובעת אילו חשבונות משתמש יכולים לשנות את ה integrity- של אובייקטים כגון קבצים, מפתחות רישום או תהליכים שבבעלות משתמשים אחרים. על ידי שינוי תווית של אובייקט שבבעלות משתמש אחר, עלול משתמש זדוני לגרום להם להריץ קוד זדוני ברמת הרשאה גבוהה יותר.
24. ההגדרה Modify firmware environment values מאפשרת למשתמשים להגדיר את משתני הסביבה הכוללים מערכות המשפיעים על תצורת החומרה. מידע זה נשמר בדרך כלל בתצורה האחרונה הידועה כטובה. שינוי ערכים אלה ועלול להוביל לכשל בחומרה שיגרום למניעת שירות.
25. ההגדרה Perform volume maintenance tasks מאפשרת למשתמשים לנהל את נפח המערכת או את תצורת הדיסק, דבר אשר יכול לאפשר למשתמש למחוק אמצעי אחסון ולגרום לאובדן נתונים וכן ליצור תנאים שימנעו מתהליכים לרוץ.
26. ההגדרה Profile single process קובעת אילו משתמשים יכולים להשתמש בכלים לניטור ביצועים של תהליכים שאינם מערכתיים. בדרך כלל, אינן צורך להגדיר את זכות המשתמש הזו לשימוש בתוסף ביצועי ה-Microsoft Management Console (MMC). עם זאת, יש צורך בהרשאת משתמש זו אם מערכת Monitor מוגדרת לאסוף נתונים באמצעות Windows Management Instrumentation (WMI). הגבלת הרשאות משתמש בתהליך יחיד בפרופיל מונעת מתוקפים להשיג מידע נוסף אשר יכול לשמש לביצוע התקפה על המערכת.
27. ההגדרה Profile system performance מאפשרת למשתמשים להשתמש בכלים כדי להציג את הביצועים של מערכות שונות ותהליכים שונים, דבר שעלול להיות מנוצל לרעה כדי לאפשר לתוקפים לקבוע את פעולת המערכת. תוקפים עם הרשאה זו יכולים לפקח על ביצועי המחשב כדי לסייע בזיהוי קריטי של תהליכים שהם עשויים לרצות לתקוף ישירות.
28. ההגדרה Replace a process level token מאפשרת לתהליך או שירות אחד להתחיל שירות או תהליך אחר עם אסימון אבטחת גישה (Access token) שונה, שניתן להשתמש בו כדי לשנות את אסימון הגישה האבטחתית של אותו תהליך משנה ולהביא להחמרת הרשאות.
29. ההגדרה Restore files and directories קובעת אילו משתמשים יכולים לעקוף הרשאות קבצים, ספריות, רישומים ואופציות קבועות אחרות בעת שחזור קבצים וספריות מגובים במחשבים המריצים את Windows Vista (או חדשים יותר) הרשאת משתמש זו קובעת גם אילו משתמשים יכולים להגדיר עקרונות אבטחה תקפים כבעלי אובייקטים; זה דומה להרשאות המשתמש בגיבוי קבצים וספריות.
30. ההגדרה shut down the system קובעת אילו משתמשים המחוברים באופן מקומי למחשבים בסביבתם יכולים לכבות את מערכת ההפעלה באמצעות פקודת כיבוי. שימוש לרעה בהרשאת משתמש זו עלולה לגרום למניעת שירות.
31. ההגדרה synchronize directory service data קובעת לאילו משתמשים וקבוצות יש סמכות לסנכרן את כל נתוני שירותי הספריות. זה ידוע גם בשם סנכרון Active Directory.
32. ההגדרה take ownership of files or other objects מאפשרת למשתמשים לקחת בעלות על קבצים, תיקיות, מפתחות רישום, או תהליכים. הרשאת משתמש זו עוקפת את כל ההרשאות הקיימות כדי להגן על אובייקטים כדי להעניק בעלות למשתמש שצוין.

המלצות לתיקון:

* מומלץ להגדיר את ההרשאה Access Credential Manager as a trusted caller ל-No one בנתיב הבא:  
  Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Access Credential Manager as a trusted caller
* מומלץ להגדיר את ההרשאה Act as part of the operating system ל-No one בנתיב הבא:  
  Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Act as part of the operating system
* מומלץ להגדיר את ההרשאה Adjust memory quotes for a process כ-Administrators, Local Service, Network Service בנתיב הבא:  
  Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Adjust memory quotas for a process
* מומלץ להגדיר את ההגדרה Back up files and directories ל-Administrators בנתיב הבא:  
  Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Back up files and directories
* מומלץ להגדיר את ההגדרה change the system time ל-Administrators, LOCAL SERVICE בנתיב הבא:  
  Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Change the system time
* מומלץ להגדיר את ההגדרה change the time zone ל-Administrators, LOCAL SERVICE בנתיב הבא:  
  Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Change the time zone
* מומלץ להגדיר את ההגדרה create a pagefile ל-Administrators בנתיב הבא:  
  Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Create a pagefile
* מומלץ להגדיר את ההרשאה Add workstations to domain לקבוצת Administrators בנתיב הבא:  
  Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Add workstations to domain
* מומלץ להגדיר את ההרשאה Create a token object ל-No one בנתיב הבא:  
  Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Create a token object
* מומלץ להגדיר את ההגדרה create global object ל-Administrators, LOCAL SERVICE, NETWORK SERVICE בנתיב הבא:  
  Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Create global objects
* מומלץ להגדיר את ההרשאה Create permanent shared objects ל-No one בנתיב הבא:  
  Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Create permanent shared objects
* מומלץ להגדיר את ההגדרה Debug programs כ-Administrators בנתיב הבא:  
  Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Debug programs
* מומלץ להגדיר את ההרשאה Deny log on as a batch job כך שיכלול את הקבוצה Guests בנתיב הבא:  
  Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Deny log on as a batch job
* מומלץ להגדיר את ההרשאה Deny log on as a service כך שיכלול את הקבוצה Guests בנתיב הבא:  
  Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Deny log on as a service
* מומלץ להגדיר את ההרשאה Deny log on locally כך שיכלול את הקבוצה Guests בנתיב הבא:  
  Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Deny log on locally
* מומלץ להגדיר את ההרשאה Deny log on through Remote Desktop Services כך שיכלול את הקבוצה Guests ואת ה-Local account בנתיב הבא:  
  Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Deny log on through Remote Desktop Services
* מומלץ להגדיר את ההגדרה Force shutdown from a remote system ל-Administrators בנתיב הבא:  
  Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Force shutdown from a remote system
* מומלץ להגדיר את ההגדרה generate security audits ל-LOCAL SERVICE, NETWORK SERVICE בנתיב הבא:  
  Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Generate security audits
* מומלץ להגדיר את ההגדרה increase scheduling priority ל-Administrators בנתיב הבא:  
  Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Increase scheduling priority
* מומלץ להגדיר את ההגדרה load and unload device drivers ל-Administrators בנתיב הבא:  
  Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Load and unload device drivers
* מומלץ להגדיר את ההרשאה Lock pages in memory ל-No one בנתיב הבא:  
  Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Lock pages in memory
* מומלץ להגדיר את ההרשאה Log on as a batch job לקבוצת ה-Administrators בנתיב הבא:  
  Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Log on as a batch job
* מומלץ להגדיר את ההרשאה Modify an object label ל-No one בנתיב הבא:  
  Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Modify an object label
* מומלץ להגדיר את ההגדרה modify firmware environment values ל-Administrators בנתיב הבא:  
  Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Modify firmware environment values
* מומלץ להגדיר את ההרשאה Perform volume maintenance tasks לקבוצת ה-Administrators בנתיב הבא:  
  Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Perform volume maintenance tasks
* מומלץ להגדיר את ההגדרה profile single process ל-Administrators בנתיב הבא:  
  Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Profile single process
* מומלץ להגדיר את ההרשאה Profile system performance לקבוצת ה-Administrators ולמשתמש NT SERVICE\WdiServiceHost בנתיב הבא:  
  Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Profile system performance
* מומלץ להגדיר את ההרשאה Replace a process level token ל-local service, network service בנתיב הבא:   
  Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Replace a process level token
* מומלץ להגדיר את ההגדרה restore files and directories ל-Administrators בנתיב הבא:  
  Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Restore files and directories
* מומלץ להגדיר את ההגדרה shut down the system ל-Administrators בנתיב הבא:  
  Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Shut down the system
* מומלץ להגדיר את ההגדרה synchronize directory service data ל-No one בנתיב הבא:  
  Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Synchronize directory service data
* מומלץ להגדיר את ההגדרה take ownership of files and other objects ל-Administrators בנתיב הבא:  
  Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Take ownership of files or other objects   
  1. ליקויים בהגדרות הרשת.

פירוט הממצא:

1. במהלך הבדיקה נמצא כ ההגדרה Microsoft network client: Digitally sign communications (always) אינה מוגדרת.
2. במהלך הבדיקה נמצא כי ההגדרה Microsoft network client: Digitally sign communications (if server agrees) אינה מוגדרת כראוי.
3. במהלך הבדיקה נמצא כי ההגדרה Microsoft network client: Send unencrypted password to third-party SMB servers אינה מוגדרת כראוי.
4. במהלך הבדיקה נמצא כי ההגדרה Microsoft network server: Amount of idle time required before suspending session אינה מוגדרת כראוי.
5. במהלך הבדיקה נמצא כי ההגדרה Microsoft network server: Digitally sign communications (always) אינה מוגדרת כראוי.
6. במהלך הבדיקה נמצא כי ההגדרה Microsoft network server: Digitally sign communications (if client agrees) אינה מוגדרת כראוי.
7. במהלך הבדיקה נמצא כי ההגדרה Microsoft network server: Disconnect clients when logon hours expire אינה מוגדרת.
8. במהלך הבדיקה נמצא כי ההגדרה Microsoft network server: Server SPN target name validation level אינה מוגדרת.
9. במהלך הבדיקה נמצא כי ההגדרה Network access: Allow anonymous SID/Name translation אינה מוגדרת כראוי.
10. במהלך הבדיקה נמצא כי ההגדרהNetwork access: Do not allow anonymous enumeration of SAM accounts אינה מוגדרת כראוי.
11. במהלך הבדיקה נמצא כי ההגדרה Network access: Do not allow anonymous enumeration of SAM accounts and shares אינה מוגדרת כראוי.
12. במהלך הבדיקה נמצא כי ההגדרה Network access: Do not allow storage of passwords and credentials for network authentication אינה מוגדרת כראוי.
13. במהלך הבדיקה נמצא כי ההגדרה Network access: Let Everyone permissions apply to anonymous users אינה מוגדרת כראוי.
14. במהלך הבדיקה נמצא כי ההגדרה Network access: Restrict anonymous access to Named Pipes and Shares אינה מוגדרת כראוי.
15. במהלך הבדיקה נמצא כי ההגדרה Network access: Restrict clients allowed to make remote calls to SAM אינה מוגדרת כראוי.
16. במהלך הבדיקה נמצא כי ההגדרה Network access: Shares that can be accessed anonymously אינה מוגדרת כראוי.
17. במהלך הבדיקה נמצא כי ההגדרה Network security: Allow Local System to use computer identity for NTLM אינה מוגדרת כראוי.
18. במהלך הבדיקה נמצא כי ההגדרה Network Security: Allow LocalSystem NULL session fallback אינה מוגדרת כראוי.
19. במהלך הבדיקה נמצא כי ההגדרה Network Security: Allow PKU2U authentication requests to this computer to use online identities אינה מוגדרת.
20. במהלך הבדיקה נמצא כי ההגדרה Network security: Configure encryption types allowed for Kerberos אינה מוגדרת.
21. במהלך הבדיקה נמצא כי ההגדרה Network security: Do not store LAN Manager hash value on next password change אינה מוגדרת כראוי.
22. במהלך הבדיקה נמצא כי ההגדרה Network security: LAN Manager authentication level אינה מוגדרת כראוי.
23. במהלך הבדיקה נמצא כי ההגדרה Network security: LDAP client signing requirements אינה מוגדרת כראוי.
24. במהלך הבדיקה נמצא כי ההגדרה Network Security: Minimum session security for NTLM SSP based (including secure RPC) clients אינה מוגדרת כראוי.
25. במהלך הבדיקה נמצא כי ההגדרה Network Security: Minimum session security for NTLM SSP based (including secure RPC) servers אינה מוגדרת כראוי.

סבירות מימוש הנזק: בינונית

חומרת הנזק: בינונית

רמת הסיכון: בינונית

פירוט הסיכון:

1. ההגדרה Microsoft network client: Digitally sign communications (always) קובעת האם נדרש לחתום את פקטות המידע על ידי לקוח ה-SMB.  
   במתקפת Session hijacking משתמשים בכלים המאפשרים לתוקפים להפריע, לסיים או לגנוב session. תוקפים עלולים ליירט ולשנות חבילות SMB אשר אינו חתומות, ולאחר מכן להעביר אותם כך שהשרת יבצע פעולות שאינן רצויות, או אפילו לאפשר גישה בלתי מורשית לנתונים.
2. ההגדרה Microsoft network client: Digitally sign communications (if server agrees) קובעת האם לקוח ה SMB ינסה לנהל משא ומתן על חתימת חבילות SMB.
3. ההגדרה Microsoft network client: Send unencrypted password to third-party SMB servers קובעת אם מפנה ה-SMB ישלח סיסמאות בטקסט רגיל במהלך האימות לשרתי ה-SMB של צד שלישי שאינם תומכים בהצפנת סיסמאות.
4. ההגדרה Microsoft network server: Amount of idle time required before suspending session מאפשרת לך לציין את משך זמן הסרק הרציף שעובר ב-session SMB לפני שההפעלה מושהית בגלל חוסר פעילות. מנהלי מערכת יכולים להשתמש בהגדרת מדיניות זו כדי לקבוע מתי מחשב יושהה עקב חוסר פעילות SMB. אם פעילות הלקוח תתחדש, ההפעלה תופעל מחדש באופן אוטומטי.
5. ההגדרה Microsoft network server: Digitally sign communications (always) קובעת אם נדרשת חתימה על חבילות על ידי רכיב שרת ה-SMB. אפשר הגדרת מדיניות זו בסביבה מעורבת כדי למנוע מלקוחות במורד הזרם להשתמש בתחנת העבודה כשרת רשת.
6. ההגדרה Microsoft network server: Digitally sign communications (if client agrees) קובעת האם שרת ה-SMB ינהל משא ומתן על חתימת חבילות ה-SMB עם הלקוחות המבקשים זאת. אם לא מגיעה בקשת חתימה מהלקוח, חיבור יתאפשר ללא חתימה עם שרת הרשת של מיקרוסופט: הגדרת חתימה דיגיטלית (תמיד) אינה מופעלת.
7. ההגדרה Microsoft network server: Disconnect clients when logon hours expire קובעת האם לנתק את המשתמשים בעת חריגה בהתחברות למחשב מעבר לשעות העבודה המוגדרות למשתמש. משתמשים אשר אינם אמורים לקבל גישה למשאבי רשת מחוץ לשעות העבודה שלהם עלולים להשתמש במשאבים אלה. בנוסף, הגדרה זו תוכל לצמצם את משטח התקיפה בכך שלא יוכלו לבצע את התקיפה בשעות שהמשתמשים אינם פעילים.
8. ההגדרה Microsoft network server: Server SPN target name validation level שולטת ברמת האימות של שמחשב מבצע בSPN המסופק על ידי הלקוח בעת הקמת session באמצעות פרוטוקול ה-SMB. ניתן לזייף את זהות המחשב כדי לקבל גישה בלתי מורשית למשאבי רשת, ולכן מומלץ להפעיל את הגדרה זו.
9. ההגדרה Network access: Allow anonymous SID/Name translation קובעת אם משתמש אנונימי יכול לבקש תכונות מזהה אבטחה (SID) עבור משתמש אחר, או להשתמש ב-SID כדי להשיג את שם המשתמש המתאים לו.
10. ההגדרה Network access: Do not allow anonymous enumeration of SAM accounts שולטת ביכולתם של משתמשים אנונימיים למנות את החשבונות במנהל חשבונות האבטחה (SAM). אם תפעיל הגדרת מדיניות זו, משתמשים עם חיבורים אנונימיים לא יוכלו למנות שמות משתמשים של חשבון תחום במערכות בסביבתך. הגדרת מדיניות זו מאפשרת גם הגבלות נוספות על קשרים אנונימיים.
11. ההגדרה Network access: Do not allow anonymous enumeration of SAM accounts and shares שולטת ביכולתם של משתמשים אנונימיים למנות חשבונות SAM כמו גם שיתופים. אם תפעיל הגדרת מדיניות זו, משתמשים אנונימיים לא יוכלו למנות שמות משתמשים של הדומיין ושמות שיתופי רשת במערכות בסביבתך.
12. ההגדרה Network access: Do not allow storage of passwords and credentials for network authentication קובעת האם ה-Credential Manager ישמור סיסמאות או פרטי הזדהות לשימוש מאוחר יותר לשימוש מאוחר יותר. לאחר התחברות למחשב, המשתמש יוכל לגשת לפרטים השמורים בזיכרון, דבר היכול להוביל לדליפת הסיסמה במידה והמשתמש מריץ קוד זדוני אשר מעביר את אותן סיסמאות למשתמש בלתי מורשה.
13. ההגדרה Network access: Let Everyone permissions apply to anonymous users קובעת אילו הרשאות נוספות מוקצות לחיבורים אנונימיים למחשב.
14. ההגדרה Network access: Restrict anonymous access to Named Pipes and Shares מגבילה גישה אנונימית רק לאותם שיתופים וצינורות הנקראים בגישה לרשת: צינורות בעלי שם שאליהם ניתן לגשת באופן אנונימי וגישה לרשת: שיתופים שניתן לגשת אליהם באופן אנונימי. הגדרת מדיניות זו שולטת בגישה של הפעלת null לשיתופים במחשבים שלך על ידי הוספת RestrictNullSessAccess עם הערך 1 במפתח HKEY\_LOCAL\_MACHINE \ System \ CurrentControlSet \ Services \ LanManServer \ Parameters. ערך רישום זה מפעיל או מכבה את שיתופי ההפעלה של null כדי לקבוע אם שירות השרת מגביל את הגישה של לקוחות לא מאומתים למשאבים.
15. ההגדרה Network access: Restrict clients allowed to make remote calls to SAM מאפשרת להגביל חיבורי RPC מרוחקים ל-SAM, על מנת להבטיח שמשתמש בלתי מורשה יוכל למנות באופן אנונימי שמות של קבוצות או משתמשים מקומיים, ולהשתמש בהם לאחר מכן על מנת לבצע מתקפות כגון Brute-Force או ישתמש בהנדסה חברתית.
16. ההגדרה Network access: Shares that can be accessed anonymously קובעת לאילו שיתופי רשת משתמשים אנונימיים יכולים לגשת. במידה ומגדירים הגדרה זו בצורה לא נכונה, משתמשים ברשת יוכלו לגשת לכלל השיתופים, דבר העלול להוביל לחשיפת מידע רגיש או השחתת נתונים.
17. ההגדרה Network security: Allow Local System to use computer identity for NTLM קובעת האם שירותי מערכת מקומיים יוכלו להשתמש בזהות המחשב בעת ניהול משא ומתן בעת אימות עם NTLM. קיימות מערכת הפעלה אשר בעת התחברות שירותי מערכת משתמשים בזהות המחשב או ב-null session, אשר באמצעותו נוצר מפתח הפעלה שאינו מספק הגנה, אך מאפשר ליישום לחתום ולהצפין נתונים ללא שגיאות.
18. הגדרת מדיניות זו קובעת אם מותר ל-NTLM לחזור להפעלה בשימוש עם LocalSystem.
19. ההגדרה Network Security: Allow PKU2U authentication requests to this computer to use online identities קובעת האם משתמשים מקוונים יכולים לבצע התחברות למחשב. הפרוטוקול PKU2U הינו פרוטוקול אימות P2P. אימות צריך להיות מנוהל באופן מרוכז, ועל כן מומלץ להשבית הגדרה זו.
20. ההגדרה Network security: Configure encryption types allowed for Kerberos מגדירה את סוגי ההצפנות בהםKerberos יוכל לממש. קיימות הצפנות אשר נחשבות חלשות ופריצות ועל כן מומלץ שלא להשתמש בהם.
21. ההגדרה Network security: Do not store LAN Manager hash value on next password change קובעת אם ערך הגיבוב של LAN Manager (LM) עבור הסיסמה החדשה נשמר בעת שינוי הסיסמה. גיבוב ה-LM חלש יחסית ונוטה להיות יותר מותקף בהשוואה לגיבוב ה-Windows NT החזק יותר מבחינה קריפטוגרפית. מאחר ש-LM מאוחסנים במחשב המקומי במאגר האבטחה, ניתן לפגוע בקלות בסיסמאות אם מסד הנתונים מותקף.
22. LM (LAN Manager) הינה קבוצה של תוכנות שרת/לקוח שאפשרה למשתמשים לקשר בין מחשבים אישיים ברשת אחת. יכולות אלה כללו שיתוף קבצים ומדפסות, תכונות אבטחה וכלי ניהול רשת.  
    מבחינת Active Directory, פרוטוקול האימות המוגדר הינו Kerberos, אך במידה ולא קיים אימות עם פרוטוקול זה, ה-AD ישתמש ב-LM, NTLM או NTLMv2. ההגדרה Network security: LAN Manager authentication level קובעת את רמת האימות של ה-LAN Manager, על ידי קביעת פרוטוקול אימות ה-challenge/response.  
    NTLMv2 משתמש בערוץ מאובטח על מנת להגן על תהליך האימות, ולמנוע הסנפת פרטי הזדהות.
23. ההגדרה Network security: LDAP client signing requirements קובעת את רמת חתימת הנתונים המתבקשת מטעם לקוחות המוציאים בקשות LDAP BIND.
24. ההגדרות Network Security: Minimum session security for NTLM SSP based (including secure RPC) מגנות על תעבורת הרשת בו משתמש ספק תמיכת האבטחה של NTLM מלהיחשף או להשתנות על ידי תוקף שקיבל גישה לאותה רשת.  
    ניתן להגיד כי הגדרות אלה מגנות מפני מתקפת MITM.

המלצות לתיקון:

* מומלץ להגדיר את ההגדרה Microsoft network client: Digitally sign communications (always) ל-Enabled בנתיב הבא:

Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Microsoft network client: Digitally sign communications (always)

* מומלץ להגדיר את ההגדרה Microsoft network client: Digitally sign communications (if server agrees) ל-Enabled בנתיב הבא:  
  Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Microsoft network client: Digitally sign communications (if server agrees)
* מומלץ להגדיר את ההגדרה Microsoft network client: Send unencrypted password to third-party SMB servers ל-Disabled בנתיב הבא:  
  Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Microsoft network client: Send unencrypted password to third-party SMB servers
* מומלץ להגדיר את ההגדרה Microsoft network server: Amount of idle time required before suspending session ל15 דקות או פחות אך לא 0 בנתיב הבא:  
  Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Microsoft network server: Amount of idle time required before suspending session
* מומלץ להגדיר את ההגדרהMicrosoft network server: Digitally sign communications (always) ל-Enabled בנתיב הבא:  
  Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Microsoft network server: Digitally sign communications (always)
* מומלץ להגדיר את ההגדרה Microsoft network server: Digitally sign communications (if client agrees) ל-Enabled בנתיב הבא:  
  Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Microsoft network server: Digitally sign communications (if client agrees)
* מומלץ להגדיר את ההגדרה Microsoft network server: Disconnect clients when logon hours expire ל-Enabled בנתיב הבא:

Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Microsoft network server: Disconnect clients when logon hours expire

* מומלץ להגדיר את ההגדרה Microsoft network server: Server SPN target name validation level כ-Accept if provided by clientבנתיב הבא:  
  Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Microsoft network server: Server SPN target name validation level
* מומלץ להגדיר את ההגדרה Network access: Allow anonymous SID/Name translation ל-Disabled בנתיב הבא:  
  Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network access: Allow anonymous SID/Name translation
* מומלץ להגדיר את ההגדרה Network access: Do not allow anonymous enumeration of SAM accounts כ-Enabled בנתיב הבא:  
  Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network access: Do not allow anonymous enumeration of SAM accounts
* מומלץ להגדיר את ההגדרה Network access: Do not allow anonymous enumeration of SAM accounts and shares ל-Enabled בנתיב הבא:  
  Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network access: Do not allow anonymous enumeration of SAM accounts and shares
* מומלץ להגדיר את ההגדרה Network access: Do not allow storage of passwords and credentials for network authentication כ-Enabled בנתיב הבא:  
  Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network access: Do not allow storage of passwords and credentials for network authentication
* מומלץ להגדיר את ההגדרה Network access: Let Everyone permissions apply to anonymous users כ-Disabled בנתיב הבא:  
  Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network access: Let Everyone permissions apply to anonymous users
* מומלץ להגדיר את ההגדרה Network access: Restrict anonymous access to Named Pipes and Shares כ-Enabled בנתיב הבא:  
  Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network access: Restrict anonymous access to Named Pipes and Shares
* מומלץ להגדיר את ההגדרה Network access: Restrict clients allowed to make remote calls to SAM כ-Administrators: Remote Access: Allow בנתיב הבא:  
  Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network access: Restrict clients allowed to make remote calls to SAM
* מומלץ להגדיר את ההגדרה Network access: Shares that can be accessed anonymously ל-None בנתיב הבא:  
  Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network access: Shares that can be accessed anonymously
* מומלץ להגדיר את ההגדרה Network security: Allow Local System to use computer identity for NTLM כ-Enabled בנתיב הבא:  
  Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network security: Allow Local System to use computer identity for NTLM
* מומלץ להגדיר את ההגדרה Network security: Allow LocalSystem NULL session fallback ל-Disabled בנתיב הבא:  
  Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network security: Allow LocalSystem NULL session fallback
* מומלץ להגדיר את ההגדרה Network Security: Allow PKU2U authentication requests to this computer to use online identities כ-Disabled בנתיב הבא:  
  Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network Security: Allow PKU2U authentication requests to this computer to use online identities
* מומלץ להגדיר את ההגדרה Network security: Configure encryption types allowed for Kerberos כ- RC4\_HMAC\_MD5, AES128\_HMAC\_SHA1, AES256\_HMAC\_SHA1, Future encryption type בנתיב הבא:  
  Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network security: Configure encryption types allowed for Kerberos
* מומלץ להגדיר את ההגדרה Network security: Do not store LAN Manager hash value on next password change ל-Enabled בנתיב הבא:  
  Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network security: Do not store LAN Manager hash value on next password change
* מומלץ להגדיר את ה- Network security: LAN Manager authentication levelל- Send NTLMv2 response only. Refuse LM & NTLM בנתיב הבא:  
  Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network security: LAN Manager authentication level
* מומלץ להגדיר את ההגדרה Network security: LDAP client signing requirements ל-Negotiate signing בנתיב הבא:  
  Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network security: LDAP client signing requirements
* מומלץ להגדיר את ה- Network security: Minimum session security for NTLM SSP based (including secure RPC) clients ל- Require NTLMv2 session security, Require 128-bit encryption בנתיב הבא:

Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network security: Minimum session security for NTLM SSP based (including secure RPC) clients.

* מומלץ להגדיר את ה- Network security: Minimum session security for NTLM SSP based (including secure RPC) servers ל- Require NTLMv2 session security, Require 128-bit encryption בנתיב הבא:

Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network security: Minimum session security for NTLM SSP based (including secure RPC) servers.

* 1. ליקויים בהגדרת יומני הביקורת.

פירוט הממצא:

במהלך הבדיקה נמצא כי Audit Log אינם מתעדים את כלל האירועים הנדרשים בתחומים הבאים:

1. Audit Credential Validation
2. Audit Application Group Management
3. Audit Computer Account Management
4. Audit Other Account Management Events
5. Audit Security Group Management
6. Audit PNP Activity
7. Audit Process Creation
8. Audit Account Lockout
9. Audit Group Membership
10. Audit Logoff
11. Audit Logon
12. Audit Other Logon/Logoff Events
13. Audit Special Logon
14. Audit Removable Storage
15. Audit Policy Change
16. Audit Authentication Policy Change
17. Audit Authorization Policy Change
18. Audit Sensitive Privilege Use
19. Audit IPsec Driver
20. Audit Other System Events
21. Audit Security State Change
22. Audit User Account Management
23. Audit Security System Extension
24. Audit System Integrity

סבירות מימוש הנזק: בינונית

חומרת הנזק: בינונית

רמת הסיכון: בינונית

פירוט הסיכון:

הקטגוריות המצוינות מעלה מדווחות על מגוון רחב של נושאים כגון אימות פרטי הזדהות לביצוע פעולות התחברות והתנתקות למערכת, נעילת חשבונות משתמשים, שינויים בקבוצות יישומים, ניהול חשבונות מחשבים וחשבונות משתמשים כגון יצירה, שינוי או מחיקה של חשבונות, ניהול קבוצות תפוצה, חיבורי התקנים חיצוניים וכו'.

כלל האירועים בתחומים המוזכרים מעלה יכולים להיות שימושיים ביותר בעת תקלה או בעת חקירת אירוע חריג במערכת.

המלצות לתיקון:

מומלץ להגדיר תיעוד אירועים בתחומים הבאים:

* Audit Credential Validation – תיעוד כישלונות והצלחות:  
  Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Account Logon\Audit Credential Validation
* Audit Application Group Management – תיעוד כישלונות והצלחות:  
  Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Account Management\Audit Application Group Management
* Audit Computer Account Management – תיעוד כישלונות והצלחות:  
  Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Account Management\Audit Computer Account Management
* Audit Other Account Management Events – תיעוד כישלונות והצלחות:  
  Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Account Management\Audit Other Account Management Events
* Audit Security Group Management – תיעוד כישלונות והצלחות:  
  Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Account Management\Audit Security Group Management
* Audit User Account Management – תיעוד כישלונות והצלחות:  
  Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Account Management\Audit User Account Management
* Audit PNP Activity – תיעוד הצלחות:  
  Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Detailed Tracking\Audit PNP Activity
* Audit Process Creation – תיעוד הצלחות:  
  Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Detailed Tracking\Audit Process Creation
* Audit Account Lockout – תיעוד כישלונות והצלחות:  
  Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Logon/Logoff\Audit Account Lockout
* Audit Group Membership – תיעוד הצלחות:  
  Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Logon/Logoff\Audit Group Membership
* Audit Logoff – תיעוד הצלחות:  
  Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Logon/Logoff\Audit Logoff
* Audit Logon – תיעוד כישלונות והצלחות:  
  Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Logon/Logoff\Audit Logon
* Audit Other Logon/Logoff Events – תיעוד כישלונות והצלחות:
* Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Logon/Logoff\Audit Other Logon/Logoff Events
* Audit Special Logon – תיעוד הצלחות:  
  Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Logon/Logoff\Audit Special Logon
* Audit Removable Storage – תיעוד כישלונות והצלחות:  
  Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Object Access\Audit Removable Storage
* Audit Audit Policy Change – תיעוד כישלונות והצלחות:  
  Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Policy Change\Audit Audit Policy Change
* Audit Authentication Policy Change – תיעוד הצלחות:  
  Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Policy Change\Audit Authentication Policy Change
* Audit Authorization Policy Change – תיעוד הצלחות:  
  Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Policy Change\Audit Authorization Policy Change
* Audit Sensitive Privilege Use – תיעוד כישלונות והצלחות:  
  Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Privilege Use\Audit Sensitive Privilege Use
* Audit IPsec Driver – תיעוד כישלונות והצלחות:  
  Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\System\Audit IPsec Driver
* Audit Other System Events – תיעוד כישלונות והצלחות:  
  Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\System\Audit Other System Events
* Audit Security State Change – תיעוד הצלחות:  
  Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\System\Audit Security State Change
* Audit User Account Management – תיעוד כישלונות והצלחות:  
  Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\System\ Audit User Account Management
* Audit Security System Extension – תיעוד כישלונות והצלחות:  
  Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\System\Audit Security System Extension
* Audit System Integrity – תיעוד כישלונות והצלחות:  
  Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\System\Audit System Integrity

* 1. ליקויים בהגדרות ה-Remote Services.

פירוט הממצא:

1. במהלך הבדיקה נמצא כי ההגדרה Restrict Remote Desktop Services users to a single Remote Desktop Services session אינה מוגדרת.
2. במהלך הבדיקה נמצא כי ההגדרה Always prompt for password upon connection אינה מוגדרת.
3. במהלך הבדיקה נמצא כי ההגדרה Require secure RPC communication אינה מוגדרת.
4. במהלך הבדיקה נמצא כי ההגדרה Set client connection encryption level אינה מוגדרת.
5. במהלך הבדיקה נמצא כי ההגדרה Set time limit for active but idle Remote Desktop Services sessions אינה מוגדרת כראוי.
6. במהלך הבדיקה נמצא כי ההגדרה Set time limit for disconnected sessions אינה מוגדרת.
7. במהלך הבדיקה נמצא כי ההגדרה Do not delete temp folders upon exit אינה מוגדרת.
8. במהלך הבדיקה נמצא כי ההגדרה Do not use temporary folders per session אינה מוגדרת.

סבירות מימוש הנזק: בינונית

חומרת הנזק: בינונית

רמת הסיכון: בינונית

פירוט הסיכון:

1. ההגדרה Restrict Remote Desktop Services users to a single Remote Desktop Services session מאפשרת להגביל משתמשים לSession אחד של Remote Desktop Services. הגדרה זו מבטיחה שמשתמשים וAdministrators שמבצעים התחברות מרוחקת לשרת, ימשיכו להשתמש באותו Session גם לאחר התנתקות והתחברות מחדש, דבר המונע יצירה של Session חדש. מומלץ להפעיל הגדרה זו מכיוון שהיא מונעת צריכת משאבים שאינה נחוצה, ומורידה את העומס מהשרת, דבר שיבטיח חווית משתמש טובה יותר.
2. ההגדרה Always prompt for password upon connection מציינת כי לאחר ביצוע התחברות מרוחקת, המשתמש נדרש להזין סיסמה.
3. ההגדרה Require secure RPC communication מציינת האם התחברות מרוחקת באמצעות RDP דורשת תקשורת RPC מאובטחת עם הלקוחות. הגדרה זו מגדילה את האבטחה בתקשורת RPC על ידי אישור בקשות מאומתות ומוצפנות בלבד.
4. ההגדרה Set client connection encryption level קובעת את מידת ההצפנה הקיימת בין הלקוחות לבין המארח בשירות ה-RDP. קיימות מספר רמות הצפנה:  
   א. High – מצפינה מידע הנשלח מהלקוח לשרת וההפך בהצפנה חזקה של 128 סיביות.   
   ב. Client Compatible – מצפינה מידע הנשלח בין הלקוח לשרת וההפך עם גודל המפתח המירבי שהלקוח תומך.  
   ג. Low – מצפינה מידע הנשלח מהלקוח לשרת ולהפך באמצעות הצפנה של 56 סיביות.
5. ההגדרה Set time limit for active but idle Remote Desktop Services sessions מאפשרת לציין את משך הזמן המרבי שבו הפעלה פעילה של שירותי שולחן עבודה מרוחק יכולה לפעול (ללא קלט משתמש) לפני שהיא מנותקת אוטומטית.
6. ההגדרה Set time limit for disconnected sessions שולטת בכמות הזמן שה-Session יישאר פעיל במידה והוא הופסק באופן בלתי צפוי, דבר היכול לבזבז משאבי מערכת. בנוסף, במידה וקיימים למשתמשים הגבלות על כמות Sessions פעילים, אי הגדרה של אפשרות זו יכול למנוע מהמשתמשים לבצע Sessions נוספים.
7. ההגדרה Do not delete temp folders upon exit מציינת האם Remote Desktop Services שומרים קבצים זמניים של משתמשים בעת ההתנתקות. מידע רגיש עלול להימצא בתוך תיקיות אלה, וגלוי למשתמשים חזקים המתחברים לאותה עמדה.
8. כברירת מחדל, שירותי ה-Remote Desktop יוצרים תיקייה זמנית על השרת המארח לכל Session פעיל. התיקיה נוצרת תחת התיקיה Temp תחת כל פרופיל משתמש, אשר נקראת על שם ה-SessionID. הגדרה זו מאפשרת למנוע את היצירה של התיקיות הזמניות לכל Session, דבר היגרום לשמירת כלל הקבצים הזמניים תחת תיקיית Temp משותפת לכלל ה-Sessions.

המלצות לתיקון:

* מומלץ להגדיר את ההגדרה Restrict Remote Desktop Services users to a single Remote Desktop Services session ל-Enabled בנתיב הבא:  
  Computer Configuration\Policies\Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Session Host\Connections\Restrict Remote Desktop Services users to a single Remote Desktop Services session
* מומלץ להגדיר את ההגדרה Always prompt for password upon connection ל-Enabled בנתיב הבא:  
  Computer Configuration\Policies\Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Session Host\Security\Always prompt for password upon connection
* מומלץ להגדיר את ההגדרה Require secure RPC communication ב-Enabled בנתיב הבא:  
  Computer Configuration\Policies\Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Session Host\Security\Require secure RPC communication
* מומלץ להגדיר את ההגדרה Set client connection encryption level ל-Enabled: High-Level בנתיב הבא:  
  Computer Configuration\Policies\Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Session Host\Security\Set client connection encryption level
* מומלץ להגדיר את ההגדרה Set time limit for active but idle Remote Desktop Services sessions ל-Enabled – 15 minutes or less בנתיב הבא:  
  Computer Configuration\Policies\Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Session Host\Session Time Limits\Set time limit for active but idle
* מומלץ להגדיר את ההגדרה Set time limit for disconnected sessions ל-Enabled: 1 minute בנתיב הבא:

Computer Configuration\Policies\Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Session Host\Session Time Limits\Set time limit for disconnected sessions

* מומלץ להגדיר את ההגדרה Do not delete temp folders upon exit ל-Disabled בנתיב הבא:  
  Computer Configuration\Policies\Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Session Host\Temporary Folders\Do not delete temp folders upon exit
* מומלץ להגדיר את ההגדרה Do not use temporary folders per session ל-Disabled בנתיב הבא:  
  Computer Configuration\Policies\Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Session Host\Temporary Folders\Do not use temporary folders per session
  1. ליקויים בהגדרות ה-Event Log.

פירוט הממצא:

במהלך הבדיקה נמצאו שני ליקויים עיקריים בקבצי הלוג בקטגוריות Application, Security, Setup ו-System:

1. ההגדרה Control Event Log behavior when the log file reaches its maximum size בכל אחת מהקטגוריות אינה מוגדרת כראוי.
2. ההגדרה Specify the maximum log file size (KB) בכל אחת מהקטגוריות אינה מוגדרת כראוי.

סבירות מימוש הנזק: בינונית

חומרת הנזק: בינונית

רמת הסיכון: בינונית

פירוט הסיכון:

1. ההגדרה Control Event Log behavior when the log file reaches its maximum size שולטת בהתנהגות יומן האירועים כאשר קובץ הלוג מגיע לגודלו המירבי. מומלץ להשבית הגדרה זו מכיוון שכשאר לא מתועדים אירועים חדשים, ייתכן שיהיה קשה או בלתי אפשרי לתחקר אירוע, לקבוע את מקור בעיה או תקלה במערכת, ואף יהיה קשה מאוד לשחזר פעילות בלתי מורשית של גורם עיון או משתמש זדוני.
2. ההגדרה Specify the maximum log file size (KB) מציינת את הגודל המירבי של קובץ הלוג ב-KB. ניתן להגדיר את קבצי הלוג בין 1MB ל-4TB.

המלצות לתיקון:

* מומלץ להגדיר את ההגדרה Control Event Log behavior when the log file reaches its maximum size כ-Disabled בנתיבים הבאים:

1. Computer Configuration\Policies\Administrative Templates\Windows Components\Event Log Service\Application\Control Event Log behavior when the log file reaches its maximum size
2. Computer Configuration\Policies\Administrative Templates\Windows Components\Event Log Service\Security\Control Event Log behavior when the log file reaches its maximum size
3. Computer Configuration\Policies\Administrative Templates\Windows Components\Event Log Service\Setup\Control Event Log behavior when the log file reaches its maximum size
4. Computer Configuration\Policies\Administrative Templates\Windows Components\Event Log Service\System\Control Event Log behavior when the log file reaches its maximum size

* מומלץ להגדיר את ההגדרה Specify the maximum log file size (KB) כ-Enabled: 32,768 or greater בנתיבים הבאים:

1. Computer Configuration\Policies\Administrative Templates\Windows Components\Event Log Service\Application\Specify the maximum log file size (KB)
2. Computer Configuration\Policies\Administrative Templates\Windows Components\Event Log Service\Security\Specify the maximum log file size (KB)
3. Computer Configuration\Policies\Administrative Templates\Windows Components\Event Log Service\Setup\Specify the maximum log file size (KB)
4. Computer Configuration\Policies\Administrative Templates\Windows Components\Event Log Service\System\Specify the maximum log file size (KB)
   1. ליקויים בהגדרות ה-WinRM.

פירוט הממצא:

1. במהלך הבדיקה נמצא כי ההגדרה Allow Basic authentication אינה מוגדרת.
2. במהלך הבדיקה נמצא כי ההגדרה Allow unencrypted traffic אינה מוגדרת.
3. במהלך הבדיקה נמצא כי ההגדרה Disallow Digest authentication אינה מוגדרת.
4. במהלך הבדיקה נמצא כי ההגדרה Allow remote server management through WinRM אינה מוגדרת.
5. במהלך הבדיקה נמצא כי ההגדרה Disallow WinRM from storing RunAs credentials אינה מוגדרת.

סבירות מימוש הנזק: בינונית

חומרת הנזק: בינונית

רמת הסיכון: בינונית

פירוט הסיכון:

1. ההגדרה Allow Basic authentication מאפשרת לנהל את ה-Windows Remote Management (WinRM) באימות בסיסי. אימות בסיסי הינו חלש על פני שיטות אחרות הקיימות ב-WinRM מכיוון שפרטי הזדהות כולל סיסמאות מועברים כ-Plaintext בטווח התקשורת. תוקף אשר מצליח להאזין לטווח עלול לתפוס פרטיםאלו ברשתולגנוב את פרטי ההזדהות בהם נעשה שימוש ב-WinRM.
2. ההגדרה Allow unencrypted traffic מאפשרת לקבוע האם לקוח יכול לשלוח ולקבל הודעות שאינן מוצפנות ברשת. הצפנת התעבורה של WinRM מפחיתה את הסיכון שתוקף יוכל להיחשף או לשנות הודעות WinRM בזמן העברתם ברשת.
3. ההגדרה Disallow Digest authentication מאפשרת לקבוע האם יתבצע שימוש בdigest authentication, אשר הינה שיטת אימות חלש יחסית לשיטות אחרות הקיימות ב-WinRM, דבר היכול לגרום לחשיפת פרטי הזדהות.
4. ההגדרה Allow remote server management through WinRM מאפשרת לנהל במידה ו-WinRM מאזין לבקשות HTTP ברשת, דרך פורט ברירת המחדל של HTTP. יש לאפשר את השימוש ב-WinRM ברשתות מהימנות ורק כאשר ניתן לעשות באמצעות IPsec.
5. ההגדרה Disallow WinRM from storing RunAs credentials שולטת בשמירת פרטי הזדהות בעת ביצוע RunAs, דבר היכול להוביל לחשיפת פרטי ההזדהות.

המלצות לתיקון:

* מומלץ להגדיר את ההגדרה Allow Basic authentication כ-Disabled בנתיב הבא:  
  Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Remote Management (WinRM)\WinRM Client\Allow Basic authentication
* מומלץ להגדיר את ההגדרה Allow unencrypted traffic כ-Disabled בנתיב הבא:  
  Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Remote Management (WinRM)\WinRM Client\Allow unencrypted traffic
* מומלץ להגדיר את ההגדרה Disallow Digest authentication כ-Enabled בנתיב הבא:  
  Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Remote Management (WinRM)\WinRM Client\Disallow Digest authentication
* מומלץ להגדיר את ההגדרה Allow remote server management through WinRM כ-Disabled בנתיב הבא:  
  Computer Configuration\Administrative Templates\Windows Components\Windows Remote Management (WinRM)\WinRM Service\Allow remote server management through WinRM
* מומלץ להגדיר את ההגדרה Disallow WinRM from storing RunAs credentials כ-Enabled בנתיב הבא:  
  Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Remote Management (WinRM)\WinRM Service\Disallow WinRM from storing RunAs credentials
  1. ליקוי בהגדרת ה-Remote Shell.

פירוט הממצא:

במהלך הבדיקה נמצא כי ההגדרה Allow Remote Shell Access אינה מוגדרת.

סבירות מימוש הנזק: בינונית

חומרת הנזק: בינונית

רמת הסיכון: בינונית

פירוט הסיכון:

ההגדרה Allow Remote Shell Access מאפשרת לנהל את תצורת הגישה מרחוק לכל ה-Shells הנתמכים להרצת פקודות וסקריפטים. מומלץ לאפשר את השימוש במעטפת ב-shell ברשתות מהימנות וכאשר ניתן לבצע שימוש בפרוטוקולים כגון IPsec.

המלצות לתיקון:

* מומלץ להגדיר את ההגדרה Allow Remote Shell Access כ-Disabled בנתיב הבא:  
  Computer Configuration\Administrative Templates\Windows Components\Windows Remote Shell\Allow Remote Shell Access  
    
    
  1. ליקויים בהגדרות ה-Internet Communication.

פירוט הממצא:

1. במהלך הבדיקה נמצא כי ההגדרה Turn off downloading of print drivers over HTTP אינה מוגדרת כראוי.
2. במהלך הבדיקה נמצא כי ההגדרה Turn off Internet Connection Wizard if URL connection is referring to Microsoft.com אינה מוגדרת כראוי.
3. במהלך הבדיקה נמצא כי ההגדרה Turn off Internet download for Web publishing and online ordering wizards אינה מוגדרת כראוי.
4. במהלך הבדיקה נמצא כי ההגדרה Turn off printing over HTTP אינה מוגדרת כראוי.
5. במהלך הבדיקה נמצא כי ההגדרה Turn off Registration if URL connection is referring to Microsoft.com אינה מוגדרת כראוי.
6. במהלך הבדיקה נמצא כי ההגדרה Turn off Search Companion content file updates אינה מוגדרת כראוי.
7. במהלך הבדיקה נמצא כי ההגדרה Turn off the ‘Order Prints’ picture task אינה מוגדרת כראוי.
8. במהלך הבדיקה נמצא כי ההגדרה Turn off the "Publish to Web" task for files and folders אינה מוגדרת כראוי.
9. במהלך הבדיקה נמצא כי ההגדרה Turn off the Windows Messenger Customer Experience Improvement Program אינה מוגדרת כראוי.
10. במהלך הבדיקה נמצא כי ההגדרה Turn off Windows Customer Experience Improvement Program אינה מגדרת כראוי.
11. במהלך הבדיקה נמצא כי ההגדרה Turn off Help Experience Improvement Program אינה מוגדרת.
12. במהלך הבדיקה נמצא כי ההגדרה Turn off Windows Error Reporting אינה מוגדרת כראוי.
13. במהלך הבדיקה נמצא כי ההגדרה Notify antivirus programs when opening attachments אינה מוגדרת כראוי.
14. במהלך הבדיקה נמצא כי ההגדרה Turn off all Windows spotlight features אינה מוגדרת.

סבירות מימוש הנזק: בינונית

חומרת הנזק: בינונית

רמת הסיכון: בינונית

פירוט הסיכון:

1. drivers הקשורים במדפסות בתווך של HTTP, דבר העלול להוביל להורדת קוד זדוני.
2. ההגדרה Turn off Internet Connection Wizard if URL connection is referring to Microsoft.com מציינת האם אשף חיבור האינטרנט יכול להתחבר ל-Microsoft על מנת להוריד רשימות של ספקי אינטרנט (ISP). מומלץ להגדיר שלא יתבצע חיבור ל-Microsoft על מנת שמשתמש לא יחשוף נתונים רגישים בלא ידיעתו.
3. ההגדרה Turn off Internet download for Web publishing and online ordering wizards קובעת אם Windows יוריד רשימות ספקים מהאינטרנט. הפעלת הגדרה זו תפחית את הסיכון שמשתמש יוריד תכנים זדוניים בלא ידיעתו.
4. ההגדרה Turn off printing over HTTP מאפשרת להשבית את יכולת מחשב הלקוח להדפיס באמצעות HTTP. מידע המועבר ב-HTTP נתון להאזנה וליירוט על ידי תוקפים.
5. ההגדרה Turn off Registration if URL connection is referring to Microsoft.com מציינת האם אשף הרישום של Windows מתחבר ל-Microsoft.com להרשמה מקוונת. מומלץ שלא להשתמש בהגדרה זו בסביבה מנוהלת.
6. ההגדרה Turn off Search Companion content file updates מציינת האם יש להוריד אוטומטית עדכוני תוכן בעת חיפושים מקומיים וחיפושים באינטרנט. קיים סיכוי שמשתמשים יחשפו מידע רגיש ללא ידעתם בשל הנושאים אותם הם מחפשים.
7. ההגדרה Turn off the ‘Order Prints’ picture task מציינת אם המשימה "הזמנת הדפסות מקוונת" זמינה ממשימות תמונה בתיקיות Windows.  
   אשף הזמנות הדפסות המקוון משמש להורדת רשימת ספקים ולאפשר למשתמשים להזמין הדפסים באופן מקוון.
8. ההגדרה Turn off the "Publish to Web" task for files and folders קובעת האם ניתן לפרסם קבצים, תיקיות או פריטים נבחרים כך שיהיו זמינים באינטרנט, דבר שיכול לגרום לפרסום של מידע רגיש או אישי ברשת.
9. ההגדרה Turn off the Windows Messenger Customer Experience Improvement Program קובעת האם ה-Windows Messenger יכול לאסוף מידע אנונימי אודות אופן השימוש בתוכנה על מנת לשפר את חוויות הלקוח.
10. ההגדרה Turn off Windows Customer Experience Improvement Program קובעת האם המשתמש יוכל לשלוח מידע אנונימי אודות שימוש באפליקציות על מנת לשפר את חווית הלקוח.
11. ההגדרה Turn off Help Experience Improvement Program מגדירה האם משתמש משתתף בתוכנית לשיפור החוויות, האוספת מידע על האופן שבו לקוחות משתמשים בעזרה של Windows כדי ש-Microsoft תוכל לשפר אותה, פעולה שיכולה לאסוף מידע על המחשבים.
12. ההגדרה Turn off Windows Error Reporting קובעת האם דיווחים על שגיאות אודות מערכת או יישום שנכשלו או הפסיקו להגיב ידווחו ל-Microsoft.
13. ההגדרה Notify antivirus programs when opening attachments מנהלת את ההתנהגות של הודעות אודות תוכניות אנטי-וירוס רשומות. במידה ותוכניות אנטי-וירוס אינן מבצעות בדיקות גישה, הן לא יוכלו לסרוק קבצים שהורדו.
14. Windows Spotlight אוספת נתונים ומשתמשת בהן כדי להציג אפליקציות מוצעות ותמונות מהאינטרנט. ההגדרה Turn off all Windows spotlight features מבטיחה כי נתונים אישיים לא ישותפו עם תוכניות צד ג'.

המלצות לתיקון:

* מומלץ להגדיר את ההגדרה Turn off downloading of print drivers over HTTP כ-Enabled בנתיב הבא:  
  Computer Configuration\Policies\Administrative Templates\System\Internet Communication Management\Internet Communication settings\Turn off downloading of print drivers over HTTP
* מומלץ להגדיר את ההגדרה Turn off Internet Connection Wizard if URL connection is referring to Microsoft.com כ-Enabled בנתיב הבא:  
  Computer Configuration\Policies\Administrative Templates\System\Internet Communication Management\Internet Communication settings\Turn off Internet Connection Wizard if URL connection is referring to Microsoft.com
* מומלץ להגדיר את ההגדרה Turn off Internet download for Web publishing and online ordering wizards כ-Enabled בנתיב הבא:  
  Computer Configuration\Policies\Administrative Templates\System\Internet Communication Management\Internet Communication settings\Turn off Internet download for Web publishing and online ordering wizards
* מומלץ להגדיר את ההגדרה Turn off printing over HTTP כ-Enabled בנתיב הבא:  
  Computer Configuration\Policies\Administrative Templates\System\Internet Communication Management\Internet Communication settings\Turn off printing over HTTP
* מומלץ להגדיר את ההגדרה Turn off Registration if URL connection is referring to Microsoft.com כ-Enabled בנתיב הבא:  
  Computer Configuration\Policies\Administrative Templates\System\Internet Communication Management\Internet Communication settings\Turn off Registration if URL connection is referring to Microsoft.com
* מומלץ להגדיר את ההגדרה Turn off Search Companion content file updates כ-Enabled בנתיב הבא:  
  Computer Configuration\Policies\Administrative Templates\System\Internet Communication Management\Internet Communication settings\Turn off Search Companion content file updates
* מומלץ להגדיר את ההגדרה Turn off the 'Order Prints' picture task ל-Enabled בנתיב הבא:  
  Computer Configuration\Policies\Administrative Templates\System\Internet Communication Management\Internet Communication settings\Turn off the "Order Prints" picture task
* מומלץ להגדיר את ההגדרה Turn off the "Publish to Web" task for files and folders ב-Enabled בנתיב הבא:  
  Computer Configuration\Policies\Administrative Templates\System\Internet Communication Management\Internet Communication settings\Turn off the "Publish to Web" task for files and folders
* מומלץ להגדיר את ההגדרה Turn off the Windows Messenger Customer Experience Improvement Program כ-Enabled בנתיב הבא:  
  Computer Configuration\Policies\Administrative Templates\System\Internet Communication Management\Internet Communication settings\Turn off the Windows Messenger Customer Experience Improvement Program
* מומלץ להגדיר את ההגדרה Turn off Windows Customer Experience Improvement Program כ-Enabled בנתיב הבא:  
  Computer Configuration\Policies\Administrative Templates\System\Internet Communication Management\Internet Communication settings\Turn off Windows Customer Experience Improvement Program
* מומלץ להגדיר את ההגדרה Turn off Help Experience Improvement Program כ-Enabled בנתיב הבא:  
  User Configuration\Policies\Administrative Templates\System\Internet Communication Management\Internet Communication Settings\Turn off Help Experience Improvement Program
* מומלץ להגדיר את ההגדרה Turn off Windows Error Reporting כ-Enabled בנתיב הבא:  
  Computer Configuration\Policies\Administrative Templates\System\Internet Communication Management\Internet Communication settings\Turn off Windows Error Reporting
* מומלץ להגדיר את ההגדרה Notify antivirus programs when opening attachments כ-Enabled בנתיב הבא:  
  User Configuration\Policies\Administrative Templates\Windows Components\Attachment Manager\Notify antivirus programs when opening attachments
* מומלץ להגדיר את ההגדרה Turn off all Windows spotlight features ל-Enabled בנתיב הבא:  
  User Configuration\Policies\Administrative Templates\Windows Components\Cloud Content\Turn off all Windows spotlight features

* 1. ליקויים בהגדרות אבטחת משתמשים וחשבונות.

פירוט הממצא:

1. במהלך הבדיקה נמצא כי ההגדרה Accounts: Administrator account status אינה מוגדרת כראוי.
2. במהלך הבדיקה נמצא כי ההגדרה Accounts: Block Microsoft accounts אינה מוגדרת כראוי.
3. במהלך הבדיקה נמצא כי ההגדרה Accounts: Guest account status אינה מוגדרת כראוי.
4. במהלך הבדיקה נמצא כי ההגדרהAudit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings אינה מוגדרת כראוי.
5. במהלך הבדיקה נמצא כי ההגדרה Audit: Shut down system immediately if unable to log security audits אינה מוגדרת כראוי.
6. במהלך הבדיקה נמצא כי ההגדרה Devices: Allowed to format and eject removable media אינה מוגדרת כראוי.
7. במהלך הבדיקה נמצא כי ההגדרה Devices: Prevent users from installing printer drivers אינה מוגדרת כראוי.
8. במהלך הבדיקה נמצא כי ההגדרה Domain member: Digitally encrypt or sign secure channel data (always) אינה מוגדרת כראוי.
9. במהלך הבדיקה נמצא כי ההגדרה Domain member: Digitally encrypt secure channel data (when possible) אינה מוגדרת כראוי.
10. במהלך הבדיקה נמצא כי ההגדרה Domain member: Digitally sign secure channel data (when possible) אינה מוגדרת כראוי.
11. במהלך הבדיקה נמצא כי ההגדרה Domain member: Disable machine account password changes אינה מוגדרת כראוי.
12. במהלך הבדיקה נמצא כי ההגדרה Domain member: Maximum machine account password age אינה מוגדרת כראוי.
13. במהלך הבדיקה נמצא כי ההגדרה Domain member: Require strong (Windows 2000 or later) session key אינה מוגדרת כראוי.

סבירות מימוש הנזק: נמוכה

חומרת הנזק: בינונית

רמת הסיכון: נמוכה

פירוט הסיכון:

* + - 1. ההגדרה Accounts: Administrator account status מאפשרת או מבטלת את חשבון מנהל המערכת במהלך פעולה רגילה. בארגונים מסוימים, שינוי סיסמה תקופתי ותדיר עבור חשבונות מקומיים עלול להוות אתר ניהולי, לכן ההמלצה היא להפוך את חשבון מנהל המערכת המובנה ל-Disabled ולהגן עליו מפני התקפה. סיבה נוספת להפוך את החשבון ל-Disable היא על מנת שלא יכול להיות נעול ולא משנה כמה כניסות כושלות הוא צובר, מה שהופך אותו למטרה עיקרית עבור התקפות Brute Force המנסות לנחש סיסמאות.
      2. ההגדרה Accounts: Block Microsoft accounts מונעת ממשתמשים להוסיף חשבונות מיקרוסופט חדשים במחשב. ארגונים המעוניינים ליישם ביעילות מדיניות ניהול זהויות ולשמור על השליטה באילו חשבונות משתמשים יהיו קיימים בכניסה למחשבים שלהם ירצו לחסום חשבונות מיקרוסופט.
      3. ההגדרה Accounts: Guest account status קובעת אם חשבון ה-Guest מופעל או מושבת. חשבון Guest מאפשר למשתמשי רשת לא מאומתים לקבל גישה למערכת.
      4. הגדרת מדיניות זו מאפשרת למנהלים לאפשר יכולות ביקורת מדויקות יותר. הגדרות מדיניות הביקורת הזמינות Windows Server 2003 Active Directoryאינן מכילות הגדרות לניהול קטגוריות המשנה החדשות לביקורת. כדי להחיל כראוי את מדיניות הביקורת שנקבעה בקו בסיס זה יש להגדיר את ההגדרה כמופעלת.
      5. ההגדרה Audit: Shut down system immediately if unable to log security audits קובעת אם המערכת תיכבה במידה ואין באפשרותה לרשום אירועי אבטחת מידע.
      6. ההגדרה Devices: Allowed to format and eject removable media קובעת מי רשאי להוציא מדית NTFS נשלפת. ניתן להשתמש בהגדרת מדיניות זו כדי למנוע ממשתמשים לא מורשים להסיר נתונים במחשב אחד כדי לגשת אליהם במחשב אחר שבו יש להם הרשאות מנהל מקומיות.
      7. ההגדרה Devices: Prevent users from installing printer drivers קובעת מי רשאי להתקין התקן מדפסת כחלק מהחיבור למדפסת משותפת. כדי שהמחשב ידפיס למדפסת משותפת, יש להתקין את מנהל ההתקן של אותה מדפסת משותפת במחשב המקומי.
      8. ההגדרה Domain member: Digitally encrypt or sign secure channel data (always) קובעת אם כל תעבורת הערוץ המאובטח שיזם משתמש הארגון הרשום חייבת להיות חתומה או מוצפנת.
      9. ההגדרה Domain member: Digitally encrypt secure channel data (when possible) קובעת האם על משתמש הארגון לנסות ליישם הצפנה עבור כל תעבורת הערוצים המאובטחת שהוא יוזם.
      10. ההגדרה Domain member: Digitally sign secure channel data (when possible) קובעת האם על משתמש הארגון לנסות ליישם חתימה דיגיטאלית והאם כל תעבורת הערוץ המאובטח שהמשתמש יוזם חייבת להיות חתומה דיגיטלית. חתימות דיגיטליות מגנות על תעבורה מפני שינויים על ידי מי שתופס את הנתונים בזמן שהוא מתקשרברשת.
      11. ההגדרה Domain member: Disable machine account password changes קובעת אם משתמש ארגון יכול לשנות מעת לעת את סיסמת חשבון המחשב שלו. מחשבים שלא יכולים לשנות באופן אוטומטי את סיסמאות החשבון שלהם עלולים להיות פגיעים מכיוון שתוקף יוכל לקבוע את הסיסמה עבור חשבון הדומיין של המערכת.
      12. ההגדרה Domain member: Maximum machine account password age קובעת את הגיל המרבי המותר לסיסמת חשבון מחשב. כברירת מחדל, משתמשי הארגון משנים אוטומטית את סיסמאות הדומיין שלהם כל 30 יום.
      13. באמצעות ההגדרה Domain member: Require strong (Windows 2000 or later) session key ניתן ליצור ערוץ מאובטח רק עם בקרי קבוצות המשתמשים המסוגלים להצפין נתוני ערוצים מאובטחים באמצעות מפתח הצפנה חזק (128 סיביות).

המלצות לתיקון:

* מומלץ להגדיר את ההגדרה Accounts: Administrator account status ל-Disabled בנתיב הבא:  
  Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Accounts: Administrator account status
* מומלץ להגדיר את ההגדרה Accounts: Block Microsoft accounts ל-Users can't add or log on with Microsoft accounts בנתיב הבא:  
  Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Accounts: Block Microsoft accounts
* מומלץ להגדיר את ההגדרה Accounts: Guest account status ל-Disables בנתיב הבא:  
  Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Accounts: Guest account status
* מומלץ להגדיר את ההגדרה ל-Enabled בנתיב הבא:  
  Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings
* מומלץ להגדיר את ההגדרה Audit: Shut down system immediately if unable to log security audits כ-Disables בנתיב הבא:  
  Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Audit: Shut down system immediately if unable to log security audits
* מומלץ להגדיר את ההגדרה Devices: Allowed to format and eject removable media ל-Administrators בנתיב הבא:  
  Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Devices: Allowed to format and eject removable media
* מומלץ להגדיר את ההגדרה Devices: Prevent users from installing printer drivers ל-Enabled בנתיב הבא:  
  Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Devices: Prevent users from installing printer drivers
* מומלץ להגדיר את ההגדרה Domain member: Digitally encrypt or sign secure channel data (always) ל-Enabled בנתיב הבא:  
  Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Domain member: Digitally encrypt or sign secure channel data (always)
* מומלץ להגדיר את ההגדרה Domain member: Digitally encrypt secure channel data (when possible) ל-Enable בנתיב הבא:  
  Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Domain member: Digitally encrypt secure channel data (when possible)
* מומלץ להגדיר את ההגדרה Domain member: Digitally sign secure channel data (when possible) ל-Enabled בנתיב הבא:  
  Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Domain member: Digitally sign secure channel data (when possible)
* מומלץ להגדיר את ההגדרה Domain member: Disable machine account password changes ל-Disabled בנתיב הבא:  
  Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Domain member: Disable machine account password changes
* מומלץ להגדיר את ההגדרה Domain member: Maximum machine account password age ל-30 ימים אך לא פחות בנתיב הבא:  
  Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Domain member: Maximum machine account password age
* מומלץ להגדיר את ההגדרה Domain member: Require strong (Windows 2000 or later) session key ל-Enabled בנתיב הבא:  
  Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Domain member: Require strong (Windows 2000 or later) session key
  1. ליקויים בהגדרות ה-Interactive Logon.

פירוט הממצא:

1. במהלך הבדיקה נמצא כי ההגדרה Interactive logon: Do not display last user name איה מוגדרת כראוי.
2. במהלך הבדיקה נמצא כי ההגדרה Interactive logon: Do not require CTRL+ALT+DEL אינה מוגדרת כראוי.
3. במהלך הבדיקה נמצא כי ההגדרה Interactive logon: Machine inactivity limit אינה מוגדרת כראוי.
4. במהלך הבדיקה נמצא כי ההגדרה Interactive logon: Require Domain Controller Authentication to unlock workstation אינה מוגדרת כראוי.
5. במהלך הבדיקה נמצא כי ההגדרה Interactive logon: Prompt user to change password before expiration אינה מוגדרת כראוי.

סבירות מימוש הנזק: נמוכה

חומרת הנזק: בינונית

רמת הסיכון: נמוכה

פירוט הסיכון:

1. ההגדרה Interactive logon: Do not display last user name קובעת אם שם החשבון של המשתמש האחרון שנכנס למחשבי הלקוח בארגון יוצג במסך הכניסהשל Windows. הפעלת הגדרה זו יכולה למנוע מתוקפים לאסוף שמות חשבונות באופן חזותי ממסכי המחשבים השולחניים והמחשבים הניידים בארגון.
2. ההגדרה Interactive logon: Do not require CTRL+ALT+DEL קובעת אם המשתמשים חייבים ללחוץ על CTRL + ALT + DEL לפני שהם נכנסים לחשבון.
3. ההגדרה Interactive logon: Machine inactivity limit מבחינה בחוסר פעילות של במערכת, ובמידה ומשך הזמן חורג מהמגבלה המצוינת בהגדרה זו, שומר המסך יפעל וינעל את המערכת.  
   אם משתמש שוכח לנעול את מחשבו, הגדרה זו יכולה למנוע מתקפות כגון Hijacking.
4. ההגדרה Interactive logon: Require Domain Controller Authentication to unlock workstation קובעת האם יש צורך ליצור קשר עם ה-DC על מנת לקבל מידע אודות המחשב כדי לבטל את נעילתו. כברירת מחדל, המחשב שומר בזיכרון את פרטי ההתחברות של המשתמשים באופן מקומי. המחשב משתמש בפרטים אלה עבור כל המשתמשים. כאשר נעשה שימוש בפרטים אלה, כל שינוי שבוצע לאחרונה בחשבון (כגון הקצאת הרשאות, נעילת חשבון או אפילו השבתתו) אינם נחשבים או מחולים עד שהחשבון מאומת.
5. ההגדרה Interactive logon: Prompt user to change password before expiration קובעת כמה זמן מראש יקבלו משתמשים אזהרה כי סיסמתם עומדת לפוג.

המלצות לתיקון:

* מומלץ להגדיר את ההגדרה Interactive logon: Do not display last user name ל-Enabled בנתיב הבא:  
  Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Interactive logon: Do not display last user name
* מומלץ להגדיר אתך ההגדרה Interactive logon: Do not require CTRL+ALT+DEL ל-Disabled בנתיב הבא:  
  Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Interactive logon: Do not require CTRL+ALT+DEL
* מומלץ להגדיר את ההגדרה Interactive logon: Machine inactivity limit בין 0 ל-900 שניות בנתיב הבא:  
  Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Interactive logon: Machine inactivity limit
* מומלץ להגדיר את ההגדרה Interactive logon: Require Domain Controller Authentication to unlock workstation כ-Enabled בנתיב הבא:  
  Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Interactive logon: Require Domain Controller Authentication to unlock workstation
* מומלץ להגדיר את ההגדרה Interactive logon: Prompt user to change password before expiration בין 5 ל-14 ימים בנתיב הבא:  
  Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Interactive logon: Prompt user to change password before expiration
  1. ליקויים בהגדרות ה-Windows Defender Firewall.

פירוט הממצא:

1. במהלך הבדיקה נמצא כי ההגדרה Prohibit installation and configuration of Network Bridge on your DNS domain network אינה מוגדרת כראוי.
2. במהלך הבדיקה נמצא כי ההגדרה Prohibit use of Internet Connection Sharing on your DNS domain network אינה מוגדרת כראוי.
3. במהלך הבדיקה נמצא כי ההגדרה Require domain users to elevate when setting a network's location אינה מוגדרת כראוי.

סבירות מימוש הנזק: נמוכה

חומרת הנזק: בינונית

רמת הסיכון: נמוכה

פירוט הסיכון:

1. ההגדרה Prohibit installation and configuration of Network Bridge on your DNS domain network מאפשרת למחשב שיש לו חיבורים לשתי רשתות שונות לחלוק נתונים בין אותן רשתות. בסביבה ארגונית, בה יש צורך לשלוט בתעבורת הרשת לנתיבים מורשים בלבד, במידה ומאפשרים למשתמשים ליצור Network bridge הדבר עלול להוביל להגדלת שטח התקיפה בידי תוקפים פוטנציאלים.
2. ההגדר Prohibit use of Internet Connection Sharing on your DNS domain network חלה על פונקציית ה-Hotspot. משתמשים בעלי הרשאות נמוכות לא אמורים להיות בעלי הרשאה להפעיל פונקציה זו ולפתוח את קישוריות האינטרנט שלהם למכשירים ניידים סמוכים.
3. ההגדרה Require domain users to elevate when setting a network's location קובעת האם בעת הגדרת מיקום הרשת יש להשתמש בהרשאות גבוהות יותר. מתן אפשרות למשתמשים רגילים לקבוע את מיקום הרשת מגדיל את משטח התקיפה.

המלצות לתיקון:

* מומלץ להגדיר את ההגדרה Prohibit installation and configuration of Network Bridge on your DNS domain network ל-Enabled בנתיב הבא:  
  Computer Configuration\Policies\Administrative Templates\Network\Network Connections\Prohibit installation and configuration of Network Bridge on your DNS domain network
* מומלץ להגדיר את ההגדרה Prohibit use of Internet Connection Sharing on your DNS domain network ל-Enabled בנתיב הבא:  
  Computer Configuration\Policies\Administrative Templates\Network\Network Connections\Prohibit use of Internet Connection Sharing on your DNS domain network
* מומלץ להגדיר את ההגדרה Require domain users to elevate when setting a network's location כ-Enabled בנתיב הבא:  
  Computer Configuration\Policies\Administrative Templates\Network\Network Connections\Require domain users to elevate when setting a network's location
  1. ליקויים בהגדרות ה-UAC.

פירוט הממצא:

1. במהלך הבדיקה נמצא כי ההגדרה User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode אינה מוגדרת כראוי.
2. במהלך הבדיקה נמצא כי ההגדרה User Account Control: Behavior of the elevation prompt for standard users אינה מוגדרת כראוי.
3. במהלך הבדיקה נמצא כי ההגדרה User Account Control: Run all administrators in Admin Approval Mode אינה מוגדרת כראוי.
4. במהלך הבדיקה נמצא כי ההגדרה User Account Control: Virtualize file and registry write failures to per-user locations אינה מוגדרת כראוי.
5. במהלך הבדיקה נמצא כי ההגדרה User Account Control: Admin Approval Mode for the Built-in Administrator account אינה מוגדרת כראוי.
6. במהלך הבדיקה נמצא כי ההגדרה User Account Control: Allow UIAccess applications to prompt for elevation without using the secure desktop אינה מוגדרת כראוי.
7. במהלך הבדיקה נמצא כי ההגדרה User Account Control: Detect application installations and prompt for elevation אינה מוגדרת כראוי.
8. במהלך הבדיקה נמצא כי ההגדרה User Account Control: Only elevate UIAccess applications that are installed in secure locations אינה מוגדרת כראוי.
9. במהלך הבדיקה נמצא כי ההגדרה User Account Control: Switch to the secure desktop when prompting for elevation אינה מוגדרת כראוי.

סבירות מימוש הנזק: נמוכה

חומרת הנזק: בינונית

רמת הסיכון: נמוכה

פירוט הסיכון:

1. ההגדרהUser Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode שולטת בהתנהגות בקשת ההרשאות עבור מנהלי מערכת. הגדרה זו מתריעה על פעולות עם הרשאות גבוהות ומאפשרת למנהל המערכת למנוע מתוכנית זדונית להסלים את הרשאותיה.
2. ההגדרה User Account Control: Behavior of the elevation prompt for standard users שולטת בהתנהגות בקשת ההרשאות עבור משתמשים רגילים.
3. ההגדרה User Account Control: Run all administrators in Admin Approval Mode שולטת בהתנהגות כל ההגדרות של UAC עבור המחשב. כלומר, במידה והגדרה זו תהיה כבויה, לא יהיה שימוש ב-UAC על העמדה.
4. ההגדרה User Account Control: Virtualize file and registry write failures to per-user locationsמגדירה אם כשלים באפליקציות מנותבים ל-Registry ולמיקומים שונים במערכת הקבצים. הגדרה זו מקלה על יישומים הרצים כ-Administrator ומצמצמת פגיעויות על ידי כתיבת מידע למיקומים מורשים בלבד.
5. ההגדרה User Account Control: Admin Approval Mode for the Built-in Administrator account שולטת בהתנהגות מצב באישור מנהלי מערכת עבור חשבון מנהל המערכת המובנה.
6. ההגדרה User Account Control: Allow UIAccess applications to prompt for elevation without using the secure desktop קובעת האם תוכניות נגישות ממשק משתמש (UIAccess או UIA) יכולות להשבית באופן אוטומטי את שולחן העבודה המאובטח לצורך הנחיות גובה המשמשות משתמש רגיל.
7. ההגדרה User Account Control: Detect application installations and prompt for elevation שולטת בהתנהגות זיהוי התקנת היישומים עבור המחשב.
8. ההגדרה User Account Control: Only elevate UIAccess applications that are installed in secure locations קובעת האם יישומים המבקשים לפעול עם רמת אמינות של נגישות ממשק משתמש (UIAccess) חייבים להימצא במיקום מאובטח במערכת הקבצים.
9. ההגדרה User Account Control: Switch to the secure desktop when prompting for elevation קובעת האם בקשת הגובה תוצג על שולחן העבודה של המשתמש האינטראקטיבי או על שולחן העבודה המאובטח.

המלצות לתיקון:

* מומלץ להגדיר את ההגדרה User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Modeכ- Prompt for consent on the secure desktop בנתיב הבא:  
  Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode
* מומלץ להגדיר את ההגדרה User Account Control: Behavior of the elevation prompt for standard users ל- Automatically deny elevation requestsבנתיב הבא:  
  Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\User Account Control: Behavior of the elevation prompt for standard users
* מומלץ להגדיר את ההגדרה User Account Control: Run all administrators in Admin Approval Mode כ-Enabled בנתיב הבא:  
  Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\User Account Control: Run all administrators in Admin Approval Mode
* מומלץ להגדיר את ההגדרה User Account Control: Virtualize file and registry write failures to per-user locations כ-Enabled בנתיב הבא:  
  Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\User Account Control: Virtualize file and registry write failures to per-user locations
* מומלץ להגדיר את ההגדרה User Account Control: Admin Approval Mode for the Built-in Administrator account כ-Enabled בנתיב הבא:  
  Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\User Account Control: Admin Approval Mode for the Built-in Administrator account
* מומלץ להגדיר את ההגדרה User Account Control: Allow UIAccess applications to prompt for elevation without using the secure desktop ל-Disabled בנתיב הבא:  
  Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\User Account Control: Allow UIAccess applications to prompt for elevation without using the secure desktop
* מומלץ להגדיר את ההגדרה User Account Control: Detect application installations and prompt for elevation לEnabled בנתיב הבא:  
  Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\User Account Control: Detect application installations and prompt for elevation
* מומלץ להגדיר את ההגדרה User Account Control: Only elevate UIAccess applications that are installed in secure locations ל-Enabled בנתיב הבא:  
  Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\User Account Control: Only elevate UIAccess applications that are installed in secure locations
* מומלץ להגדיר את ההגדרה User Account Control: Switch to the secure desktop when prompting for elevation ב-Enabled בנתיב הבא:  
  Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\User Account Control: Switch to the secure desktop when prompting for elevation
  1. ליקויים בהגדרות ה-Microsoft Edge.

פירוט הממצא:

1. במהלך הבדיקה נמצא כי ההגדרה Allow Extensions אינה מוגדרת כראוי.
2. במהלך הבדיקה נמצא כי ההגדרה InPrivate Browsing אינה מוגדרת.
3. במהלך הבדיקה נמצא כי ההגדרה Configure Cookies אינה מוגדרת.
4. במהלך הבדיקה נמצא כי ההגדרה Configure Password Manager אינה מוגדרת.
5. במהלך הבדיקה נמצא כי ההגדרה Configure Popup Blocker אינה מוגדרת.
6. במהלך הבדיקה נמצא כי ההגדרה search suggestions in Address bar אינה מוגדרת.
7. במהלך הבדיקה נמצא כי ההגדרה Windows Defender SmartScreen אינה מוגדרת.
8. במהלך הבדיקה נמצא כי ההגדרה Prevent Access to the about:flags page אינה מוגדרת.
9. במהלך הבדיקה נמצא כי ההגדרה Prevent Bypassing SmartScreen prompts for files אינה מוגדרת.
10. במהלך הבדיקה נמצא כי ההגדרה Prevent Bypassing SmartScreen prompts for sites אינה מוגדרת.
11. במהלך הבדיקה נמצא כי ההגדרה Don't allow WebRTC to share the LocalHost IP address אינה מוגדרת.

סבירות מימוש הנזק: נמוכה

חומרת הנזק: בינונית

רמת הסיכון: נמוכה

פירוט הסיכון:

1. ההגדרה Allow Extensions מאפשרת לקבוע אם עובדים יכולים לטעון הרחבות ב-Microsoft Edge.
2. ההגדרה InPrivate Browsing מונעת אחסון של היסטוריה, קבצי Cookie, קבצי אינטרנט זמניים או נתונים אחרים. השבתת ההגדרה מאפשרתלשמור נתונים אלה במידה ויעלה הצורך בהם.
3. ההגדרה Configure Cookies מאפשרת למשתמש להגדיר כיצד לעבוד עם Cookies ומאילו אתרים לחסום אותם. במידה ולא מחילים הגדרה ספציפית, Cookies יאופשרו מכלל האתרים.
4. ההגדרה של Password Manager מאפשרת שמירת סיסמאות לשימוש בעת גלישה. אפשרות זאת עלולה להרחיב את משטח התקיפה, ועל כן מומלץ להשביתה.
5. Popup-Block מאפשר למשתמש להגדיר מדיניות אודות חלונות קופצים.
6. search suggestions in Address bar מאפשרת למשתמש לקבל הצעות חיפוש בשורת הכתובות של Microsoft Edge.
7. מערכת SmartScreen מסייעת בהגנה על מחשבים אישיים על ידי אזהרת המשתמש לפני הפעלת תוכניות זדוניות שהורדו מהאינטרנט. אזהרה זו מוצגת כדו-שיח לפני הפעלת אפליקציה שהורדה מהאינטרנט ואינה מוכרת או אשר ידועה כזדונית.
8. הדף about:flags של Microsoft Edge מכיל אפשרויות מתקדמות ואפשרויות ניסיוניות שמפתחים יכולים לבדוק כדי לבנות דפדפן טוב יותר, דבר היכול להשפיע לרעה על הביצועים והפונקציונליות של Microsoft Edge.
9. Windows Defender SmartScreen מתריע על הורדת קבצים שאינם מאומתים. הפעלת ההגדרה Prevent Bypassing SmartScreen prompts for files משמעה כי משתמשים לא יכולים להתעלם מהאזהרות של Windows Defender, וכי הם לא יוכלו להוריד קבצים שאינם מאומתים.
10. Windows Defender SmartScreen מתריע על גישה לאתרים שעלולים להיות זדוניים. הפעלת ההגדרה Prevent Bypassing SmartScreen prompts for sites משמעה כי משתמשים לא יוכלו להתעלם מהאזהרות של Windows Defender, וכי הם לא יוכלו לגלוש באתרים שאינם מאושרים.
11. ההגדרה Don't allow WebRTC to share the LocalHost IP address מאפשרת למשתמש להחליט אם כתובת ה-Local Host IP מוצגת בעת ביצוע שיחת טלפון באמצעות פרוטוקול WebRTC.

המלצות לתיקון:

* מומלץ להגדיר את ההגדרה Allow Extensions ל-Disabled בנתיב הבא:  
  Computer Configuration\Policies\Administrative Templates\Windows Components\Microsoft Edge\Allow Extensions
* מומלץ להגדיר את ה-InPrivate Browsing ל-Disable בנתיב הבא:  
  Computer Configuration\Policies\Administrative Templates\Windows Components\Microsoft Edge\Allow InPrivate Browsing
* מומלץ להגדיר את ה-Cookies ל- Block only 3rd-party cookies בנתיב הבא:  
  Computer Configuration\Policies\Administrative Templates\Windows Components\Microsoft Edge\Configure cookies
* מומלץ להגדיר את ה-Password Manager ל-Disable בנתיב הבא:  
  Computer Configuration\Policies\Administrative Templates\Windows Components\Microsoft Edge\Configure Password Manager
* מומלץ להגדיר את ה-Popup Blocker ל-Enabled בנתיב הבא:  
  Computer Configuration\Policies\Administrative Templates\Windows Components\Microsoft Edge\Configure Pop-up Blocker
* מומלץ להגדיר את ה- search suggestions in Address bar ל-Disabled בנתיב הבא:  
  Computer Configuration\Policies\Administrative Templates\Windows Components\Microsoft Edge\Configure search suggestions in Address bar
* מומלץ להגדיר את ה-Windows Defender SmartScreen כ-Enabled בנתיב הבא:  
  Computer Configuration\Policies\Administrative Templates\Windows Components\Microsoft Edge\Configure SmartScreen Filter
* מומלץ להגדיר את ה-Prevent Access to the about:flags page ל-Enabled בנתיב הבא:  
  Computer Configuration\Policies\Administrative Templates\Windows Components\Microsoft Edge\Prevent access to the about:flags page in Microsoft Edge
* מומלץ להגדיר את ה- Prevent Bypassing SmartScreen prompts for files ל-Enabled:  
  Computer Configuration\Policies\Administrative Templates\Windows Components\Microsoft Edge\Prevent bypassing SmartScreen prompts for files
* מומלץ להגדיר את ה- Prevent Bypassing SmartScreen prompts for sites ל-Enabled:  
  Computer Configuration\Policies\Administrative Templates\Windows Components\Microsoft Edge\Prevent bypassing SmartScreen prompts for sites
* מומלץ להגדיר את ה- Prevent using Localhost IP address for WebRTC ל-Enabled:  
  Computer Configuration\Policies\Administrative Templates\Windows Components\Microsoft Edge\Prevent using Localhost IP address for WebRTC
  1. ליקויים בהגדרות ה-Logon.

פירוט הממצא:

1. במהלך הבדיקה נמצא כי ההגדרה Block user from showing account details on sign-in אינה מוגדרת כראוי.
2. במהלך הבדיקה נמצא כי ההגדרה Do not display network selection UI אינה מוגדרת כראוי.
3. במהלך הבדיקה נמצא כי ההגדרה Do not enumerate connected users on domain-joined computers אינה מוגדרת כראוי.
4. במהלך הבדיקה נמצא כי ההגדרה Enumerate local users on domain-joined computers אינה מוגדרת כראוי.
5. במהלך הבדיקה נמצא כי ההגדרה Turn off app notifications on the lock screen אינה מוגדרת כראוי.
6. במהלך הבדיקה נמצא כי ההגדרה Turn on convenience PIN sign-in אינה מוגדרת כראוי.

סבירות מימוש הנזק: נמוכה

חומרת הנזק: בינונית

רמת הסיכון: נמוכה

פירוט הסיכון:

1. ההגדרה Block user from showing account details on sign-in מונעת הצגת פרטי חשבון, כגון כתובת דואר או שם משתמש, במסך ההזדהות.  
   תוקף עם גישה לעמדה יכול להציג את שם המשתמש האחרון שהזדהה ולבצע תקיפות כגון Brute-Force או מתקפות מילון, על מנת לנחש את הסיסמה.
2. ההגדרה Do not display network selection UI מאפשרת לקבוע אם מישהו יכול לקיים אינטראקציה עם מסך הכניסה של ממשקי משתמש ברשתות הזמינות. משתמש שאינו מורשה יכול לנתק את המחשב מהרשת או לחבר את המחשב לרשתות זמינות אחרות מבלי להתחבר ל-Windows.
3. ההגדרה Do not enumerate connected users on domain-joined computers מונעת ממשתמשים מחוברים למנות את המחשבים המחוברים ל-Domain. תוקפים יכולים לנצל אפשרות זו על מנת לאסוף שמות חשבונות של משתמשים, ולאחר מכן להשתמש במידע זה בשילוב עם מתקפות כגון Brute-Force או הנדסה חברתית.
4. ההגדרה Enumerate local users on domain-joined computers מאפשרת למשתמשים מקומיים להימנות במחשבים המחוברים ל-Domain. תוקפים יכולים לנצל אפשרות זו על מנת לאסוף שמות חשבונות של משתמשים, ולאחר מכן להשתמש במידע זה בשילוב עם מתקפות כגון Brute-Force או הנדסה חברתית.
5. ההגדרה Turn off app notifications on the lock screen מאפשרת הופעת התראות של אפליקציות על מסך הנעילה. התראות אלו עלולות להציג נתונים רגישים או עסקיים ועל כן מומלץ שלא לאפשר אותן.
6. ההגדרה Turn on convenience PIN sign-in קובעת האם משתמש יכול להזדהות ל-Domain באמצעות PIN. PIN נוצר לרוב ממבחר קטןשל תווים, ולפעמים עלול להכיל רק ספרות, כך שברוב המקרים PIN יהיה פחות חזק מסיסמה רגילה.

המלצות לתיקון:

* מומלץ להגדיר את ההגדרה Block user from showing account details on sign-in כ-Enabled בנתיב הבא:  
  Computer Configuration\Policies\Administrative Templates\System\Logon\Block user from showing account details on sign-in
* מומלץ להגדיר את ההגדרה Do not display network selection UI כ-Enabled בנתיב הבא:  
  Computer Configuration\Policies\Administrative Templates\System\Logon\Do not display network selection UI
* מומלץ להגדיר את ההגדרה Do not enumerate connected users on domain-joined computers כ-Enabled בנתיב הבא:  
  Computer Configuration\Policies\Administrative Templates\System\Logon\Do not enumerate connected users on domain-joined computers
* מומלץ להגדיר את ההגדרה Enumerate local users on domain-joined computers כ-Disabled בנתיב הבא:  
  Computer Configuration\Policies\Administrative Templates\System\Logon\Enumerate local users on domain-joined computers
* מומלץ להגדיר את ההגדרה Turn off app notifications on the lock screen כ-Enabled בנתיב הבא:  
  Computer Configuration\Policies\Administrative Templates\System\Logon\Turn off app notifications on the lock screen
* מומלץ להגדיר את ההגדרה Turn on convenience PIN sign-in כ-Disabled בנתיב הבא:  
  Computer Configuration\Policies\Administrative Templates\System\Logon\Turn on convenience PIN sign-in
  1. ליקויים בהגדרות ה-Time Provider.

פירוט הממצא:

1. במהלך הבדיקה נמצא כי ההגדרה Enable Windows NTP Client אינה מוגדרת כראוי.
2. במהלך הבדיקה נמצא כי ההגדרה Enable Windows NTP Server אינה מוגדרת כראוי.

סבירות מימוש הנזק: נמוכה

חומרת הנזק: בינונית

רמת הסיכון: נמוכה

פירוט הסיכון:

1. ההגדרה Enable Windows NTP Client מאפשרת לסנכרן את שעון המחשב עם שרתי NTP אחרים. חישוב זמן אמין ומדויק חשוב למספר שירותים. השימוש ב-NTP מבטיח דיוק תפקודי.
2. ההגדרה Enable Windows NTP Server מציינת אם שרת ה-NTP מופעל. לתצורה של סנכרון זמן נכון יש חשיבות מכרעת בסביבה מנוהלת הן בשל חותמות הזמן של Kerberos והן על מנת לחולל לוגים ורישום אבטחתי מדויק.

המלצות לתיקון:

* מומלץ להגדיר את ההגדרה Enable Windows NTP Client כ-Enabled בנתיב הבא:  
  Computer Configuration\Policies\Administrative Templates\System\Windows Time Service\Time Providers\Enable Windows NTP Client
* מומלץ להגדיר את ההגדרה Enable Windows NTP Server כ-Disabled בנתיב הבא:  
  Computer Configuration\Policies\Administrative Templates\System\Windows Time Service\Time Providers\Enable Windows NTP Server
  1. ליקויים בהגדרות ה-Data Collection.

פירוט הממצא:

1. במהלך הבדיקה נמצא כי ההגדרה Allow Telemetry אינה מוגדרת כראוי.
2. במהלך הבדיקה נמצא כי ההגדרה Disable pre-release features or settings אינה מוגדרת כראוי.
3. במהלך הבדיקה נמצא כי ההגדרה Do not show feedback notifications אינה מוגדרת כראוי.
4. במהלך הבדיקה נמצא כי ההגדרה Toggle user control over Insider builds אינה מוגדרת כראוי.

סבירות מימוש הנזק: נמוכה

חומרת הנזק: בינונית

רמת הסיכון: נמוכה

פירוט הסיכון:

1. ההגדרה Allow Telemetry קובעת את כמות הנתונים המדווחים ל-Microsoft. שליחת נתונים לספק צד שלישי מהווה תמיד צעד שאינו מאובטח, ויש לעשות זאת רק בעת הצורך. ההגדרה המומלצת מגדירה שליחת נתונים מינימליים ל-Microsoft.
2. ההגדרה Disable pre-release features or settings קובעת את הרמה בה Microsoft יכולה לבחון מוצר כדי לחקור את העדפות המשתמש או התנהגות המכשיר. מומלץ שלא לאפשר הגדרה שכזאת מכיוון שהדבר יכול להוביל לתקלות ופערי אבטחה במערכת.
3. ההגדרה Do not show feedback notifications מאפשרת לארגון למנוע הצגה של שאלות משוב מבית Microsoft במכשירים.
4. ההגדרה Toggle user control over Insider builds קובעת האם משתמשים יכולים לגשת ל-Insider Builds עבור אפשרויות מתקדמות בעדכוני מערכת ההפעלה, דבר המאפשר למשתמשים להפוך את המכשירים שלהם לזמינים להורדה והתקנת תוכנת תצוגה מקדימה של Windows.

המלצות לתיקון:

* מומלץ להגדיר את ההגדרה Allow Telemetry כ- Enabled: 0 - Security [Enterprise Only] בנתיב הבא:

Computer Configuration\Policies\Administrative Templates\Windows Components\Data Collection and Preview Builds\Allow Telemetry

* מומלץ להגדיר את ההגדרה Disable pre-release features or settings כ-Disabled בנתיב הבא:  
  Computer Configuration\Policies\Administrative Templates\Windows Components\Data Collection and Preview Builds\Disable pre-release features or settings
* מומלץ להגדיר את ההגדרה Do not show feedback notifications כ-Enabled בנתיב הבא:  
  Computer Configuration\Policies\Administrative Templates\Windows Components\Data Collection and Preview Builds\Do not show feedback notifications
* מומלץ להגדיר את ההגדרה Toggle user control over Insider builds כ-Disabled בנתיב הבא:  
  Computer Configuration\Policies\Administrative Templates\Windows Components\Data Collection and Preview Builds\Toggle user control over Insider builds
  1. ליקויים בהגדרות ה-Windows Installer.

פירוט הממצא:

1. במהלך הבדיקה נמצא כי ההגדרה Allow user control over installs אינה מוגדרת.
2. במהלך הבדיקה נמצא כי ההגדרה Prevent Internet Explorer security prompt for Windows Installer scripts אינה מוגדרת.
3. במהלך הבדיקה נמצא כי ההגדרה Sign-in last interactive user automatically after a system-initiated restart אינה מוגדרת כראוי.
4. במהלך הבדיקה נמצא כי ההגדרה Always install with elevated privileges אינה מוגדרת.

סבירות מימוש הנזק: נמוכה

חומרת הנזק: בינונית

רמת הסיכון: נמוכה

פירוט הסיכון:

1. ההגדרה Allow user control over installs קובעת האם משתמש רשאי לשנות אפשרויות התקנה, אשר זמינות בדרך כלל רק למנהלי המערכת. בסביבה מנוהלת, רק צוותים מורשים צריכים לאפשר התקנה או לשנות תוכנות במערכת. מתן אפשרות למשתמשים לשלוט בהתקנות עלול לסכן בהתקנה או מחיקה של תוכנות לא מאושרות.
2. ההגדרה Prevent Internet Explorer security prompt for Windows Installer scripts קובעת האם תוכניות מבוססות אינטרנט מורשות להתקין תוכנות במחשב מבלי ליידע את המשתמש, דבר העלול להוות סיכון ולהגדיל את משטח התקיפה במערכת.
3. ההגדרה Sign-in last interactive user automatically after a system-initiated restart קובעת אם מכשיר ייכנס אוטומטית למשתמש האינטראקטיבי האחרון לאחר שה- Windows Update מפעיל מחדש את המערכת.
4. ההגדרה Always install with elevated privileges קובעת האם ה-Installer ישתמש בהרשאות מערכת בעת התקנת תוכנית. משתמשים בעלי הרשאות מוגבלות יכולים לנצל תכונה זו על ידי יצירת חבילת התקנה של Installer היוצרת חשבון מקומי חדש כחלק מקבוצה מובנית של מנהלי מערכת מקומיים, ובאמצעותו יוכלו להתקין תוכנות זדוניות או לבצע פעילויות בלתי מורשות.

המלצות לתיקון:

* מומלץ להגדיר את ההגדרה Allow user control over installs ב-Disabled בנתיב הבא:  
  Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Installer\Allow user control over installs
* מומלץ להגדיר את הגדרה Prevent Internet Explorer security prompt for Windows Installer scripts כ-Disabled בנתיב הבא:  
  Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Installer\Prevent Internet Explorer security prompt for Windows Installer scripts
* מומלץ להגדיר את ההגדרה Sign-in last interactive user automatically after a system-initiated restart כ-Disabled בנתיב הבא:  
  Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Logon Options\Sign-in last interactive user automatically after a system-initiated restart
* מומלץ להגדיר את ההגדרה Always install with elevated privileges כ-Disabled בנתיב הבא:  
  Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Installer\Always install with elevated privileges
  1. ליקויים בהגדרות ה-Windows Powershell.

פירוט הממצא:

1. במהלך הבדיקה נמצא כי ההגדרה Turn on PowerShell Script Block Logging אינה מוגדרת.
2. במהלך הבדיקה נמצא כי ההגדרה Turn on PowerShell Transcription אינה מוגדרת.

סבירות מימוש הנזק: נמוכה

חומרת הנזק: בינונית

רמת הסיכון: נמוכה

פירוט הסיכון:

1. ההגדרה Turn on PowerShell Script Block Logging מאפשרת רישום של קלט סקריפט ליומני הלוג של Microsoft-Windows-PowerShell/Operational. ברירת המחדל של ACL ביומני הלוג של Powershell מאפשרת לכל משתמש מחובר לקרוא אותו, ולכן עלולה לגרום להדלפת סיסמאות או מידע רגיש אחר למשתמשים בלתי מורשים.
2. ההגדרה Turn on PowerShell Transcription מאפשרת ללכוד את הקלט והפלט של פקודות Powershell לתמלילים מבוססי טקסט, דבר היכול להוביל לאחסון של סיסמאות או מידע רגיש בקובץ הפלט Powershell\_transcript.

המלצות לתיקון:

* מומלץ להגדיר את ההגדרה Turn on PowerShell Script Block Logging כ-Disabled בנתיב הבא:  
  Computer Configuration\Policies\Administrative Templates\Windows Components\Windows PowerShell\Turn on PowerShell Script Block Logging
* מומלץ להגדיר את ההגדרה Turn on PowerShell Transcription כ-Disabled בנתיב הבא:  
  Computer Configuration\Policies\Administrative Templates\Windows Components\Windows PowerShell\Turn on PowerShell Transcription
  1. ליקויים בהגדרות ה-Personalization.

פירוט הממצא:

1. במהלך הבדיקה נמצא כי ההגדרה Enable screen saver אינה מוגדרת.
2. במהלך הבדיקה נמצא כי ההגדרה Force specific screen saver: Screen saver executable name אינה מוגדרת.
3. במהלך הבדיקה נמצא כי ההגדרה Password protect the screen saver אינה מוגדרת.
4. במהלך הבדיקה נמצא כי ההגדרה Screen saver timeout אינה מוגדרת.
5. במהלך הבדיקה נמצא כי ההגדרה Turn off toast notifications on the lock screen אינה מוגדרת.
6. במהלך הבדיקה נמצא כי ההגדרה Prevent enabling lock screen camera אינה מוגדרת.

סבירות מימוש הנזק: נמוכה

חומרת הנזק: בינונית

רמת הסיכון: נמוכה

פירוט הסיכון:

1. ההגדרה Enable screen saver מאפשרת את השימוש בשומר מסך. במידה ומשתמש שכח לנעול את מחשבו, ייתכן שתוקף יוכל לבצע Hijacking. קביעת שומר מסך מתוזמן עם נעילת סיסמה יכולה למנוע סוג מתקפות זה.
2. ההגדרה Force specific screen saver: Screen saver executable name קובעת את שומר המסך של המשתמש.
3. ההגדרה Password protect the screen saver קובעת האם שומרי המסך המשומשים במחשב מוגנים באמצעות סיסמה.
4. ההגדרה Screen saver timeout כמה זמן צריך לעבור עד להופעת שומר המסך.
5. ההגדרה Turn off toast notifications on the lock screen מכבה את התראות ה-toast על מסך הנעילה. התראות אלה עלולות להציג מידע עסקי או אישי אודות משתמשים.
6. ההגדרה Prevent enabling lock screen camera מונעת את הפעלת המצלמה במסך הנעילה.

המלצות לתיקון:

* מומלץ להגדיר את ההגדרה Enable screen saver כ-Enabled בנתיב הבא:  
  User Configuration\Policies\Administrative Templates\Control Panel\Personalization\Enable screen saver
* מומלץ להגדיר את ההגדרה Force specific screen saver: Screen saver executable name כ- Enabled: scrnsave.scr בנתיב הבא:  
  User Configuration\Policies\Administrative Templates\Control Panel\Personalization\Force specific screen saver
* מומלץ להגדיר את ההגדרה Password protect the screen saver ל-Enabled בנתיב הבא:  
  User Configuration\Policies\Administrative Templates\Control Panel\Personalization\Password protect the screen saver
* מומלץ להגדיר את ההגדרה Screen saver timeout ל- Enabled: 900 seconds or fewer, but not 0 בנתיב הבא:  
  User Configuration\Policies\Administrative Templates\Control Panel\Personalization\Screen saver timeout
* מומלץ להגדיר את ההגדרה Turn off toast notifications on the lock screen ל-Enabled בנתיב הבא:  
  User Configuration\Policies\Administrative Templates\Start Menu and Taskbar\Notifications\Turn off toast notifications on the lock screen
* מומלץ להגדיר את ההגדרה Prevent enabling lock screen camera כ-Enabled בנתיב הבא:  
  Computer Configuration\Policies\Administrative Templates\Control Panel\Personalization\Prevent enabling lock screen camera
  1. ליקויים בהגדרות ספק הרשת.

פירוט הממצא:

1. במהלך הבדיקה נמצא כי ההגדרה Hardened UNC Paths אינה מוגדרת כראוי.
2. במהלך הבדיקה נמצא כי ההגדרה Configuration of wireless settings using Windows Connect Now אינה מוגדרת כראוי.
3. במהלך הבדיקה נמצא כי ההגדרה Prohibit access of the Windows Connect Now wizards אינה מוגדרת כראוי.
4. במהלך הבדיקה נמצא כי ההגדרה Minimize the number of simultaneous connections to the Internet or a Windows Domain אינה מוגדרת כראוי.
5. במהלך הבדיקה נמצא כי ההגדרה Prohibit connection to non-domain networks when connected to domain authenticated network אינה מוגדרת כראוי.

סבירות מימוש הנזק: נמוכה

חומרת הנזק: נמוכה

רמת הסיכון: נמוכה

פירוט הסיכון:

1. ההגדרה Hardened UNC Paths מגדירה גישה מאובטחת לנתיבי ה-UNC.
2. ההגדרה Configuration of wireless settings using Windows Connect Now מאפשרת להגדיר הגדרות אלחוטיות באמצעות WCN, המאפשר גילוי ותצורה של מחשבים דרך Ethernet. השבתת הגדרה זו משפרת את האטבחה ומפיחתה את הסיכון לתקיפת המחשב.
3. ההגדרה Prohibit access of the Windows Connect Now wizards אוסרת את הגישה ל-WCN, אשר מצמצם את משטח התקיפה.
4. ההגדרה Minimize the number of simultaneous connections to the Internet or a Windows Domain מונעת ממחשבים ליצור חיבורים מרובים בו זמנית לאינטרנט או ל-Domain, דבר המאפשר למנוע זרימת תעבורת רשת בין האינטרנט לרשת המנוהלת בארגון.
5. ההגדרה Prohibit connection to non-domain networks when connected to domain authenticated network מונעת ממחשבים להתחבר לרשת מבוססת Domain ולרשת אשר אינה מבוססת Domain בו זמנית, דבר המאפשר זרימת תעבורת רשת בין רשת ציבורית שאינה בטוחה ורשת הארגון.

המלצות לתיקון:

* מומלץ להגדיר את ההגדרה Hardened UNC Paths כך:  
  \\\*\NETLOGON RequireMutualAuthentication=1, RequireIntegrity=1

\\\*\SYSVOL RequireMutualAuthentication=1, RequireIntegrity=1

בנתיב הבא:  
Computer Configuration\Policies\Administrative Templates\Network\Network Provider\Hardened UNC Pathsr

* מומלץ להגדיר את ההגדרה Configuration of wireless settings using Windows Connect Now כ-Disabled בנתיב הבא:  
  Computer Configuration\Policies\Administrative Templates\Network\Windows Connect Now\Configuration of wireless settings using Windows Connect Now
* מומלץ להגדיר את ההגדרה Prohibit access of the Windows Connect Now wizards כ-Enabled בנתיב הבא:  
  Computer Configuration\Policies\Administrative Templates\Network\Network\Windows Connect Now\Prohibit access of the Windows Connect Now wizards
* מומלץ להגדיר את ההגדרה Minimize the number of simultaneous connections to the Internet or a Windows Domain כ-Enabled בנתיב הבא:  
  Computer Configuration\Policies\Administrative Templates\Network\Windows Connection Manager\Minimize the number of simultaneous connections to the Internet or a Windows Domain
* מומלץ להגדיר את ההגדרה Prohibit connection to non-domain networks when connected to domain authenticated network כ-Enabled בנתיב הבא:  
  Computer Configuration\Policies\Administrative Templates\Network\Windows Connection Manager\Prohibit connection to non-domain networks when connected to domain authenticated network
  1. ליקויים בהגדרות תהליכים.

פירוט הממצא:

1. במהלך הבדיקה נמצא כי ההגדרה Include command line in process creation events אינה מוגדרת כראוי.
2. במהלך הבדיקה נמצא כי ההגדרה Configure registry policy processing: Do not apply during periodic background processing אינה מוגדרת כראוי.
3. במהלך הבדיקה נמצא כי ההגדרה Configure registry policy processing: Process even if the Group Policy objects have not changed אינה מוגדרת כראוי.

סבירות מימוש הנזק: נמוכה

חומרת הנזק: נמוכה

רמת הסיכון: נמוכה

פירוט הסיכון:

1. ההגדרה Include command line in process creation events מגדירה איזה מידע מתועד בעת יצירת תהליך חדש. כאשר מדיניות זו מופעלת, כל משתמש שיש לו הרשאת קריאה לאירועים המתועדים יכול לקרוא את הארגומטים בשורת הפקודה אודות תהליכים חדשים שנוצרו, דבר העלול להכיל מידע רגיש הכולל סיסמאות או פרטי התחברות.
2. ההגדרה Configure registry policy processing: Do not apply during periodic background processing מונעת מהמערכת לעדכן את המדיניות המושפעת בקרע בזמן שימוש במחשב. כאשר עדכוני הרקע מושבתים, שינויים לא יכנסו לתוקף עד להפעלה מחדש או התחברות מחדש.
3. ההגדרה Configure registry policy processing: Process even if the Group Policy objects have not changed מתעדכנת ומחילה מדיניות מחדש גם אם המדיניות לא השתנתה. הגדרה זו מבטיחה ששינויים לא מורשים שהוגדרו באופן מקומי ישונו מחדש להגדרות ה-GPOב-Domain.

המלצות לתיקון:

* מומלץ להגדיר את ההגדרה Include command line in process creation events כ-Disabled בנתיב הבא:  
  Computer Configuration\Policies\Administrative Templates\System\Audit Process Creation\Include command line in process creation events
* מומלץ להגדיר את ההגדרה Configure registry policy processing: Do not apply during periodic background processing כ- Enabled: FALSE בנתיב הבא:  
  Computer Configuration\Policies\Administrative Templates\System\Group Policy\Configure registry policy processing
* מומלץ להגדיר את ההגדרה Configure registry policy processing: Process even if the Group Policy objects have not changed כ-Enabled:TRUE בנתיב הבא:  
  Computer Configuration\Policies\Administrative Templates\System\Group Policy\Configure registry policy processing
  1. ליקויים בהגדרות ה-Sleep.

פירוט הממצא:

1. במהלך הבדיקה נמצא כי ההגדרה Allow network connectivity during connected-standby (plugged in) אינה מוגדרת כראוי.
2. במהלך הבדיקה נמצא כי ההגדרה Require a password when a computer wakes (plugged in) אינה מוגדרת כראוי.

סבירות מימוש הנזק: נמוכה

חומרת הנזק: נמוכה

רמת הסיכון: נמוכה

פירוט הסיכון:

1. ההגדרה Allow network connectivity during connected-standby (plugged in) מאפשרת לשלוט בהגדרות הרשת במצב שינה. ההגדרה מבטיחה כי המחשב לא יהיה נגיש לתוקפים דרך רשת WLAN כשהוא נותר במצב שינה.
2. ההגדרה Require a password when a computer wakes (plugged in) מציינת האם המשתמש יתבקש להזין סיסמה ביציאה ממצב שינה. הפעלת ההגדרה מבטיחה שכל משתמש שישתמש במחשב לאחר מצב שינה יצטרך להזין פרטי הזדהות מחדש.

המלצות לתיקון:

* מומלץ להגדיר את ההגדרה Allow network connectivity during connected-standby (plugged in) כ-Disabled בנתיב הבא:   
  Computer Configuration\Policies\Administrative Templates\System\Power Management\Sleep Settings\Allow network connectivity during connected-standby (plugged in)
* מומלץ להגדיר את ההגדרה Require a password when a computer wakes (plugged in) כ-Enabled בנתיב הבא:  
  Computer Configuration\Policies\Administrative Templates\System\Power Management\Sleep Settings\Require a password when a computer wakes (plugged in)
  1. ליקויים בהגדרות ה-RPC.

פירוט הממצא:

1. במהלך הבדיקה נמצא כי ההגדרה Enable RPC Endpoint Mapper Client Authentication אינה מוגדרת כראוי.
2. במהלך הבדיקה נמצא כי ההגדרה Restrict Unauthenticated RPC clients אינה מוגדרת כראוי.

סבירות מימוש הנזק: נמוכה

חומרת הנזק: נמוכה

רמת הסיכון: נמוכה

פירוט הסיכון:

1. ההגדרה Enable RPC Endpoint Mapper Client Authentication קובעת האם לקוחות RPC מאומתים באמצעות ה-Endpoint Mapper Service כאשר השיחה שהם מבצעים מכילה פרטי אימות. גישה אנונימית לשירותי RPC עלולה לגרום לגילוי מידע למשתמשים לא מאומתים.
2. ההגדרה Restrict Unauthenticated RPC clients שולטת באופן טיפול שרת ה-RPCבלקוחות לא מאומתים המתחברים לשרת. הגדרה זו עלולה להשפיע על מגוון רחב של פעולות כולל עיבוד ה-GPO עצמו. תקשורת RPC שאינה מאומתת יכולה ליצור פגיעות.

המלצות לתיקון:

* מומלץ להגדיר את ההגדרה Enable RPC Endpoint Mapper Client Authentication כ-Enabled בנתיב הבא:  
  Computer Configuration\Policies\Administrative Templates\System\Remote Procedure Call\Enable RPC Endpoint Mapper Client Authentication
* מומלץ להגדיר את ההגדרה Restrict Unauthenticated RPC clients כ-Enabled: Authenticated בנתיב הבא:  
  Computer Configuration\Policies\Administrative Templates\System\Remote Procedure Call\Restrict Unauthenticated RPC clients
  1. ליקויים בהגדרות ה-AutoPlay.

פירוט הממצא:

1. במהלך הבדיקה נמצא כי ההגדרה Disallow Autoplay for non-volume devices אינה מוגדרת כראוי.
2. במהלך הבדיקה נמצא כי ההגדרה Set the default behavior for AutoRun אינה מוגדרת כראוי.
3. במהלך הבדיקה נמצא כי ההגדרה Turn Off AutoPlay אינה מוגדרת כראוי.

סבירות מימוש הנזק: נמוכה

חומרת הנזק: נמוכה

רמת הסיכון: נמוכה

פירוט הסיכון:

1. ההגדרה Disallow Autoplay for non-volume devices אינה מאפשרת הפעלה אוטומטית למכשירי MTP כגון מצלמות וטלפונים. תוקף יכול להשתמש בהגדרה זו על מנת להפעיל תוכנית ולפגוע במחשב או בנתונים בו.
2. ההגדרה Set the default behavior for AutoRun מגדירה את התנהגות ברירת המחדל עבור פקודות autorun. פקודות אלה נשמרות בדרך כלל בקבצים autoru.inf. בעבר, כאשר מדיה הכוללת פקודות autorun הייתה מוכנסת, המערכת ביצעה את הפקודות באופן אוטומטי ללא שום התערבות, דבר שהוביל להרצת קוד ללא ידיעת המשתמש. על כן, ההגדרה המומלצת הינה לא להריץ שום פקודות autorun.
3. ההגדרה Turn off AutoPlay שולטת על קריאה מכונן בעת הכנסת מדיה לכונן, מה שגורם לקובץ ההתקנה של תוכניות או מדית שמע להתחיל לפעול מיד. תוקף יכול להשתמש בתכונה זו כדי להפעיל תוכנית לפגוע במחשב או בנתונים במחשב. הפעלה אוטומטית מושבתת כברירת מחדל בכמה סוגי כוננים נשלפים, כגון תקליטונים וכונני רשת, אך לא בכונני תקליטורים.

המלצות לתיקון:

* מומלץ להגדיר את ההגדרה Disallow Autoplay for non-volume devices כ-Enabled בנתיב הבא:  
  Computer Configuration\Policies\Administrative Templates\Windows Components\AutoPlay Policies\Disallow Autoplay for non-volume devices
* מומלץ להגדיר את ההגדרה Set the default behavior for AutoRun כ- Enabled: Do not execute any autorun commands בנתיב הבא:  
  Computer Configuration\Policies\Administrative Templates\Windows Components\AutoPlay Policies\Set the default behavior for AutoRun
* מומלץ להגדיר את ההגדרה trun off AutoPlay ל-Enabled בנתיב הבא:  
  Computer Configuration\Policies\Administrative Templates\Windows Components\AutoPlay Policies\Turn off Autoplay
  1. ליקויים בהגדרות ה-Credential UI.

פירוט הממצא:

1. במהלך הבדיקה נמצא כי ההגדרה Do not display the password reveal button אינה מוגדרת כראוי.
2. במהלך הבדיקה נמצא כי ההגדרה Enumerate administrator accounts on elevation אינה מוגדרת כראוי.

סבירות מימוש הנזק: נמוכה

חומרת הנזק: נמוכה

רמת הסיכון: נמוכה

פירוט הסיכון:

1. ההגדרה Do not display the password reveal button מאפשרת להגדיר את כפתור גילוי הסיסמה. תכונה זו באה לידי שימוש בעת הזנת סיסמה ארוכה במיוחד ומורכבת. הסיכון הוא שמשתמש אחר עשוי לראות את הסיסמה תוך כדי התבוננות במסך.
2. ההגדרה Enumerate administrator accounts on elevation קובעת אם משתמשי מנהל מוצגים כאשר משתמש מנסה להעלות את הרשאותיו בעת הרצת יישום. מומלץ להשבית הגדרה זו מכיוון שמשתמשים יוכלו לראות את שמות חשבונות המנהלים, מה שיאפשר להם לבצע מתקפות כגוןBrute-Force על מנת לפצח את הסיסמה.

המלצות לתיקון:

* מומלץ להגדיר את ההגדרה Do not display the password reveal button כ-Enabled בנתיב הבא:  
  Computer Configuration\Policies\Administrative Templates\Windows Components\Credential User Interface\Do not display the password reveal button
* מומלץ להגדיר את ההגדרה Enumerate administrator accounts on elevation כ-Disabled בנתיב הבא:  
  Computer Configuration\Policies\Administrative Templates\Windows Components\Credential User Interface\Enumerate administrator accounts on elevation
  1. ליקויים בהגדרות הגרסאות קודמות.

פירוט הממצא:

1. במהלך הבדיקה נמצא כי ההגדרה Turn off Data Execution Prevention for Explorer אינה מוגדרת כראוי.
2. במהלך הבדיקה נמצא כי ההגדרה Turn off heap termination on corruption אינה מוגדרת כראוי.
3. במהלך הבדיקה נמצא כי ההגדרה Turn off shell protocol protected mode אינה מוגדרת כראוי.

סבירות מימוש הנזק: נמוכה

חומרת הנזק: נמוכה

רמת הסיכון: נמוכה

פירוט הסיכון:

1. ההגדרה Turn off Data Execution Prevention for Explorer יכולה לאפשר ל-Plugins מסוימים מגרסה קודמת לתפקד מבלי לעצור את ה-Explorer. מניעת הרצת נתונים היא תכונת אבטחה חשובה הנתמכת על ידי Explorer, אשר מסייעת להגביל את ההשפעה של סוגים מסוימים של תוכנות זדוניות.
2. ההגדרה Turn off heap termination on corruption לא מאפשרת ליישומי Plugin מגרסאות קודמות לתפקד כאשר ה-session של ה-Explorer נקטע. נתינת האפשרות ליישומים לתפקד לאחר שה-session נקטע מגדילה את הסיכון לתקיפת המערכת.
3. ההגדרה Turn off shell protocol protected mode מגדירה את הפונקציונליות של פרוטוקול ה-shell. שימוש בפונקציונליות מלאה מאפשרת ליישומים לפתוח תיקיות ולהפעיל קבצים. מומלץ להגביל את הפונקציונליות של פרוטוקול זה על מנת לצמצם את משטח התקיפה של המערכת.

המלצות לתיקון:

* מומלץ להגדיר את ההגדרה Turn off Data Execution Prevention for Explorer כ-Disabled בנתיב הבא:  
  Computer Configuration\Policies\Administrative Templates\Windows Components\File Explorer\Turn off Data Execution Prevention for Explorer
* מומלץ להגדיר את ההגדרה Turn off heap termination on corruption כ-Disabled בנתיב הבא:  
  Computer Configuration\Policies\Administrative Templates\Windows Components\File Explorer\Turn off heap termination on corruption
* מומלץ להגדיר את ההגדרה Turn off shell protocol protected mode כ-Disabled בנתיב הבא:  
  Computer Configuration\Policies\Administrative Templates\Windows Components\File Explorer\Turn off shell protocol protected mode
  1. ליקויים בהגדרות ה-Windows Search.

פירוט הממצא:

1. במהלך הבדיקה נמצא כי ההגדרה Allow Cortana אינה מוגדרת.
2. במהלך הבדיקה נמצא כי ההגדרה Allow Cortana above lock screen אינה מוגדרת.
3. במהלך הבדיקה נמצא כי ההגדרה Allow indexing of encrypted files אינה מוגדרת.
4. במהלך הבדיקה נמצא כי ההגדרה Allow search and Cortana to use location אינה מוגדרת.

סבירות מימוש הנזק: נמוכה

חומרת הנזק: נמוכה

רמת הסיכון: נמוכה

פירוט הסיכון:

1. ההגדרה Allow Cortana קובעת האם המשתמש יכול לתקשר עם Cortana.
2. ההגדרה Allow Cortana above lock screen קובעת האם המשתמש יכול לתקשר עם Cortana בזמן שהמערכת נעולה.
3. ההגדרה Allow indexing of encrypted files קובעת האם קבצים מוצפנים נכללים בIndex.  
   יצירת Indexing ונתינת האפשרות לחפש בו קבצים מוצפנים עלול לחשוף נתונים חסויים בתוך קבצים אלה.
4. ההגדרה Allow search and Cortana to use location מציינת האם Cortana וחיפוש יכולים לספק את המיקום הרלוונטי לתוצאות, דבר היכול להוביל תוקף למידע אודות מיקומים.

המלצות לתיקון:

* מומלץ להגדיר את ההגדרה Allow Cortana כ-Disabled בנתיב הבא:  
  Computer Configuration\Policies\Administrative Templates\Windows Components\Search\Allow Cortana
* מומלץ להגדיר את ההגדרה Allow Cortana above lock screen כ-Disabled בנתיב הבא:  
  Computer Configuration\Policies\Administrative Templates\Windows Components\Search\Allow Cortana above lock screen
* מומלץ להגדיר את ההגדרה Allow indexing of encrypted files כ-Disabled בנתיב הבא:  
  Computer Configuration\Policies\Administrative Templates\Windows Components\Search\Allow indexing of encrypted files
* מומלץ להגדיר את ההגדרה Allow search and Cortana to use location כ-Disabled בנתיב הבא:  
  Computer Configuration\Policies\Administrative Templates\Windows Components\Search\Allow search and Cortana to use location
  1. ליקויים בהגדרות ה-WindowsStore.

פירוט הממצא:

1. במהלך הבדיקה נמצא כי ההגדרה Disable all apps from Microsoft Store אינה מוגדרת.
2. במהלך הבדיקה נמצא כי ההגדרה Turn off Automatic Download and Install of updates אינה מוגדרת.
3. במהלך הבדיקה נמצא כי ההגדרה Turn off the offer to update to the latest version of Windows אינה מוגדרת.
4. במהלך הבדיקה נמצא כי ההגדרה Turn off the Store application אינה מוגדרת.

סבירות מימוש הנזק: נמוכה

חומרת הנזק: נמוכה

רמת הסיכון: נמוכה

פירוט הסיכון:

1. ההגדרה Disable all apps from Microsoft Store אחראית על השבתתשל כל האפליקציות מחנות Microsoft שהגיעו מותקנות מראש או שהורדו. כלומר, אפליקציות לא יעודכנו, וה-Store יושבת גם הוא.
2. ההגדרה Turn off Automatic Download and Install of updates מציינת האם הורדה והתקנה אוטומטית של עדכוני אפליקציות יקרו במערכת. הפעלת ההגדרה משמעה שעדכונים אוטומטים יושבתו.
3. ההגדרה turn off the offer to update to the latest version of Windows מציינת האם ה-Store יציע עדכונים לגרסה האחרונה של Windows. עדכוני מערכת לא מבוקרים יכולים לגרום לבעיות לא צפויות. עדכונים לגרסה האחרונה של Windows צריכה להתבצע בצורה נכונה ולא דרך החנות.
4. ההגדרה Turn off the Store application מגדירה האם ניתן לגשת לחנות האפליקציות.

המלצות לתיקון:

* מומלץ להגדיר את ההגדרה Disable all apps from Microsoft Store ל-Enabled בנתיב הבא:  
  Computer Configuration\Policies\Administrative Templates\Windows Components\Store\Disable all apps from Windows Store
* מומלץ להגדיר את ההגדרה Turn off Automatic Download and Install of updates ל-Disabled בנתיב הבא:  
  Computer Configuration\Policies\Administrative Templates\Windows Components\Store\Turn off Automatic Download and Install of updates
* מומלץ להגדיר את ההגדרה turn off the offer to update to the latest version of Windows כ-Enabled בנתיב הבא:  
  Computer Configuration\Policies\Administrative Templates\Windows Components\Store\Turn off the offer to update to the latest version of Windows
* מומלץ להגדיר את ההגדרה Turn off the Store application ל-Enabled בנתיב הבא:  
  Computer Configuration\Policies\Administrative Templates\Windows Components\Store\Turn off the Store application
  1. ליקויים בהגדרות ה-Windows Updates.

פירוט הממצא:

1. במהלך הבדיקה נמצא כי ההגדרה Select when Quality Updates are received אינה מוגדרת.
2. במהלך הבדיקה נמצא כי ההגדרה Configure Automatic Updates אינה מוגדרת.
3. במהלך הבדיקה נמצא כי ההגדרה No auto-restart with logged on users for scheduled automatic updates installations אינה מוגדרת.

סבירות מימוש הנזק: נמוכה

חומרת הנזק: נמוכה

רמת הסיכון: נמוכה

פירוט הסיכון:

1. ההגדרה Select when Quality Updates are received שולטת בקבלת Quality Updates, היכולים להכיל תיקוני באגים או תיקוני אבטחה חשובים, אשר יש להתקינם בהקדם האפשרי.
2. ההגדרה Configure Automatic Updates קובעת אם מחשבים יקבלו עדכוני אבטחה מ-Windows Update או WSUS, כלומר ברגע שקיים חיבור רשת זמין, מערכת הפעלה תשתמש בחיבור זה על מנת לחפש עדכונים באתר האינטרנט המיועד או ב-Windows Update. דבר זה יכול להבטיח כי תמיד יותקנו עדכוני מערכת הפעלה. יש לציין מתי מחשבים יקבלו עדכוני אבטחה.
3. ההגדרה No auto-restart with logged on users for scheduled automatic updates installations מציינת כי עדכונים אוטומטיים יחכו ל-restart על ידי המשתמש המחובר על מנת להשלים את ההתקנה המתוזמנת. חלק מעדכוני התוכנה דורשים הפעלה מחדש על מנת להשלים את העדכון, כך שאם פעולה זו לא תתבצע, הדבר יכול להוביל לעיכוב בעדכון ולהשארת מערכת ההפעלה בצורה שאינה מאובטחת.

המלצות לתיקון:

* מומלץ להגדיר את ההגדרה Select when Quality Updates are received כ-Enabled: 0 days בנתיב הבא:  
  Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Update\Defer Windows Updates\Select when Quality Updates are received
* מומלץ להגדיר את ההגדרה Configure Automatic Updates כ-Enabled בנתיב הבא:  
  Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Update\Configure Automatic Updates  
  מומלץ להגדיר את ההגדרה Configure Automatic Updates: Scheduled install day ל-0 – Every Day בנתיב הבא:  
  Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Update\Configure Automatic Updates: Scheduled install day
* מומלץ להגדיר את ההגדרה No auto-restart with logged on users for scheduled automatic updates installations כ-Disabled בנתיב הבא:  
  Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Update\No auto-restart with logged on users for scheduled automatic updates installations
  1. ליקויי אבטחה נוספים.

פירוט הממצא:

1. במהלך הבדיקה נמצא כי ההגדרה Prevent the usage of OneDrive for file storage אינה מוגדרת.
2. במהלך הבדיקה נמצא כי ההגדרה Do not allow passwords to be saved אינה מוגדרת כראוי.
3. במהלך הבדיקה נמצא כי ההגדרה Do not allow COM port redirection אינה מוגדרת כראוי.
4. במהלך הבדיקה נמצא כי ההגדרה Do not allow drive redirection אינה מוגדרת כראוי.
5. במהלך הבדיקה נמצא כי ההגדרה Do not allow LPT port redirection אינה מוגדרת כראוי.
6. במהלך הבדיקה נמצא כי ההגדרה Do not allow supported Plug and Play device redirection אינה מוגדרת כראוי.
7. במהלך הבדיקה נמצא כי ההגדרה Prevent downloading of enclosures אינה מוגדרת כראוי.
8. במהלך הבדיקה נמצא כי ההגדרה Turn off KMS Client Online AVS Validation אינה מוגדרת.
9. במהלך הבדיקה נמצא כי ההגדרה Join Microsoft MAPS אינה מוגדרת.
10. במהלך הבדיקה נמצא כי ההגדרה Configure Watson Events אינה מוגדרת.
11. במהלך הבדיקה נמצא כי הגדרות הקשורות ל-Windows Ink אינן מוגדרות.
12. במהלך הבדיקה נמצא כי ההגדרה Prevent users from sharing files within their profile אינה מוגדרת.
13. במהלך הבדיקה נמצא כי ההגדרה Prevent Codec Download אינה מוגדרת.
14. במהלך הבדיקה נמצא כי ההגדרה Turn off multicast name resolution אינה מוגדרת כראוי.
15. במהלך הבדיקה נמצא כי ההגדרה Enable Font Providers אינה מוגדרת כראוי.
16. במהלך הבדיקה נמצא כי ההגדרה Untrusted Font Blocking אינה מוגדרת כראוי.
17. במהלך הבדיקה נמצא כי ההגדרה Enable insecure guest logons אינה מוגדרת.
18. במהלך הבדיקה נמצא כי ההגדרה Turn on Mapper I/O (LLTDIO) driver אינה מוגדרת.
19. במהלך הבדיקה נמצא כי ההגדרה Turn on Responder (RSPNDR) driver אינה מוגדרת.
20. במהלך הבדיקה נמצא כי ההגדרה Turn Off Microsoft Peer-to-Peer Networking Services אינה מוגדרת כראוי.
21. במהלך הבדיקה נמצא כי ההגדרה Continue experiences on this device אינה מוגדרת כראוי.
22. במהלך הבדיקה נמצא כי ההגדרה Turn off background refresh of Group Policy אינה מוגדרת כראוי.
23. במהלך הבדיקה נמצא כי ההגדרה Support device authentication using certificate אינה מוגדרת כראוי.
24. במהלך הבדיקה נמצא כי ההגדרה Disallow copying of user input methods to the system account for sign-in אינה מוגדרת כראוי.
25. במהלך הבדיקה נמצא כי ההגדרה Configure Solicited Remote Assistance אינה מוגדרת כראוי.
26. במהלך הבדיקה נמצא כי ההגדרה Microsoft Support Diagnostic Tool: Turn on MSDT interactive communication with support provider אינה מוגדרת כראוי.
27. במהלך הבדיקה נמצא כי ההגדרה Turn off the advertising ID אינה מוגדרת כראוי.
28. במהלך הבדיקה נמצא כי ההגדרה Allow Microsoft accounts to be optional אינה מוגדרת כראוי.
29. במהלך הבדיקה נמצא כי ההגדרה Block launching Windows Store apps with Windows Runtime API access from hosted content אינה מוגדרת כראוי.
30. במהלך הבדיקה נמצא כי ההגדרה Use enhanced anti-spoofing when available אינה מוגדרת כראוי.
31. במהלך הבדיקה נמצא כי ההגדרה Allow Use of Camera אינה מוגדרת כראוי.
32. במהלך הבדיקה נמצא כי ההגדרה Turn off Microsoft consumer experiences אינה מוגדרת כראוי.
33. במהלך הבדיקה נמצא כי ההגדרה Require pin for pairing אינה מוגדרת כראוי.
34. במהלך הבדיקה נמצא כי ההגדרה Turn off location אינה מוגדרת כראוי.
35. במהלך הבדיקה נמצא כי ההגדרה Shutdown: Allow system to be shut down without having to log on אינה מוגדרת כראוי.
36. במהלך הבדיקה נמצא כי ההגדרה Turn off access to the Store אינה מוגדרת כראוי.
37. במהלך הבדיקה נמצא כי ההגדרה Configure Offer Remote Assistance אינה מוגדרת כראוי.
38. במהלך הבדיקה נמצא כי ההגדרה Enable/Disable PerfTrack אינה מוגדרת כראוי.
39. במהלך הבדיקה נמצא כי ההגדרה Do not preserve zone information in file attachments אינה מוגדרת כראוי.
40. במהלך הבדיקה נמצא כי ההגדרות Let Windows apps אינן מוגדרות כראוי.

סבירות מימוש הנזק: נמוכה

חומרת הנזק: נמוכה

רמת הסיכון: נמוכה

פירוט הסיכון:

ההגדרה Prevent the usage of OneDrive for file storage מונעת ממשתמשים להעלות בטעות מידע עסקי או רגיש לשירות הענן של OneDrive באמצעות Next Generation Sync.

הגדרה Do not allow password to be saved עוזרת למנוע שמירה של סיסמאות מחשב במצב של עבודה ב-RDP. .  
יש לציין כי אם הגדרת מדיניות זו הוגדרה בעבר כלא זמינה או לא הוגדרה, סיסמאות שנשמרו בעבר יימחקו בפעם הראשונה שמשתמש ב-RDP יתנתק משרת כלשהו.

ההגדרה Prevent downloading of enclosures מונעת מהמשתמש הורדת קבצים מצורפים מה-feed למחשב המשתמש.

ההגדרה Do not allow COM port redirection מציינת אם למנוע הפניית נתונים ליציאות COM של משתמש RDP .

ההגדרה Do not allow drive redirection מונעת ממשתמשים לשתף את הכוננים המקומיים במחשבי הלקוח שלהם לשרתים שאליהם הם ניגשים בחיבור RDP. כוננים ממופים מופיעים בעץ תיקיות ההפעלה בסייר הקבצים של Windows.

ההגדרה Do not allow LPT port redirection מציינת אם למנוע הפניית נתונים ליציאות LPT של משתמש במהלך RDP Session.

ההגדרה Do not allow supported Plug and Play device redirection מאפשרת לשלוט בניתוב מחדש של התקני Plug and Play הנתמכים, כגון התקנים ניידים של Windows, למחשב המרוחק בהפעלה של RDP.

* + - 1. KMS (Key Management Service) היא שיטה להפעלת רישיונות של Microsoft שכוללת הגדרת שרת מקומי לאחסון רישיונות התוכנה. ההגדרה Turn off KMS Client Online AVS Validation מאפשרת לבטל הסכמה לשליחת נתוני הפעלה של ה-KMS ל-Microsoft באופן אוטומטי.
      2. Microsoft MAPS הינה קהילה מקוונת המסייעת לבחור כיצד להגיב לאיומים ולעצור את ההתפשטות של תוכנות זדוניות. ניתן לאפשר שליחת מידע על תוכנות שזוהו, דבר המסייע ל-Microsoft ליצור מודיעין אבטחה חדש ולהגן על המחשב בצורה טובה יותר. יש לציין כי המידע יכול לכלול מידע כגון מיקומים של הפריטים במחשב, או מידע אישי שעלול להישלח ל-Microsoft. המידע נאסף ונשלח בצורה אוטומטית.
      3. Watson Events הם דוחות הנשלחים ל-Microsoft כאשר תוכנית או שירות במחשב קורסים או נכשלים, דבר היכול לגרום לפגיעה בפרטיות.
      4. Windows Ink Workspace מאפשר להשתמש במחשב בדומה לעבודה עם דף ועט וליצור פתקים דביקים, לצייר על לוח לבן ולשתף מידע לעולם כולו. Windows Ink משולב באפליקציות כמו מפות, Microsoft Edge ו-Office.
      5. ההגדרה Prevent users from sharing files within their profile קובעת האם משתמשים יכולים לשתף קבצים בפרופיל שלהם. משתמשים עלולים לשתף נתונים רגישים עם משתמשים לא מורשים. הארגון צריך לספק מיקום מנוהל לשיתוף קבצים.
      6. ההגדרה Prevent Codec Download קובעת אם Media Player רשאי להוריד רכיבי codec נוספים לפענוח קבצי מדיה שאינם מזוהים.
      7. ההגדרה Turn off multicast name resolution מתייחסת לפרוטוקול LLMNR. LLMNR הוא פרוטוקול לפתרון שם משני. בעת שימוש ב-LLMNR, שאילתות נשלחות באמצעות שידור לקבוצה דרך קישור רשת מקומית ברשת משנה אחת ממחשב לקוח למחשב לקוח אחר באותה רשת משנה שגם בה מופעל LLMNR. LLMNR אינו דורש שרת DNS או תצורת לקוח DNS ומספק רזולוציית שמות בתרחישים בהם אין אפשרות לפתור שמות DNS קונבנציונליים. תוקף עלול להאזין לבקשות אלה, לענות להם ולתמרן את העמדה ואת המשתמשים.
      8. ההגדרה Enable Font Providers קובעת אם ל-Windows מותר להוריד גופנים ומידע על גופנים מספקי גופנים מקוונים. בסביבה מנוהלת, מומלץ לבטל אפשרות זו על מנת להבטיח שכל השינויים נבדקים ומאושרים.
      9. ההגדרה Untrusted Font Blocking מספקת הגדרה גלובלית כדי למנוע מתוכניות לטעון גופנים לא מהימנים ,אשר הינם כל הגופנים שלא מותקנים בתיקיית %windir%\Fonts, על מנת למנוע תקיפות EoP מרוחקות או מקומיות.
      10. ההגדרה Enable insecure guest logons קובעת האם לקוח SMB יאשר התחברויות בלתי מאובטחות לשרת ה-SMB. כניסות משתמשי אורח בלתי מאובטחות משמשות שרתי קבצים כדי לאפשר גישה לא מאומתת לתיקיות משותפות.
      11. ההגדרה Turn on Mapper I/O (LLTDIO) driver אחראית על תפעוליות פרוטוקול הרשת Mapper I/O. LLTDIO מאפשרת למחשב לגלות את טופולוגיית הרשת אליה הוא מחובר. בנוסף, הוא מאפשר למחשב ליזום בקשות QoS. מומלץ להשבית אפשרות זו על מנת לסייע בהגנה מפני גילוי פוטנציאלי והתחברות למכשירים לא מורשים.
      12. ההגדרה Turn on Responder (RSPNDR) driver אחראית על תפעוליות הפרוטוקול Responder, אשר מאפשר למחשב להשתתף בבקשות גילוי טופולוגיה של שכבת ה-Link, כך שניתן יהיה לאתר אותו ברשת. מומלץ להשבית אפשרות זו על מנת לסייע בהגנה מפני גילוי פוטנציאלי והתחברות למכשירים לא מורשים.
      13. פרוטוקול רזולוציה של שם עמיתים (PNRP) מאפשר רזולוציה מבוזרת של שם לכתובת IPv6 ומספר פורט. הפרוטוקול פועל בהקשר למחשוב ענן. ענן הוא קבוצה של מחשבי עמיתים שיכולים לתקשר אחד עם השני באמצעות אותו היקף IPv6 .  
          פרוטוקולי עמית לעמית מאפשרים יישומים בתחומי RTC, שיתוף פעולה, הפצת תוכן ועיבוד מבוזר.
      14. ההגדרה Continue experiences on this device קובעת האם מכשיר רשאי להשתמש בחוויות חוצות פלטפורמה, דבר המאפשר לגשת לאפליקציות ולשלוח הודעות למכשירים אחרים.
      15. ההגדרה Turn off background refresh of Group Policy מונעת את עדכון ה-GPO בעת שימוש במחשב. הגדרה זו מבטיחה ששינויים ב-GPO ייכנסו לתוקף מהר יותר, וכי לא יהיה צורך להמתין להפעלה מחדש או התחברות מחדש למחשב.
      16. ההגדרה Support device authentication using certificate מאפשרת להגדיר תמיכה עבור Kerberos לניסיון אימות באמצעות תעודות של המכשיר ל-Domain. אימות חזק יותר להתקנים עם שימוש בתעודות הינו מאובטח יותר מאשר שימוש בשם משתמש וסיסמה.
      17. ההגדרה Disallow copying of user input methods to the system account for sign-in מונעת העתקה אוטומטית לשדה הקלט במסך ההזדהות. הגדרה זו יכולה להגביר את רמת האבטחה במערכת.
      18. ההגדרה Configure Solicited Remote Assistance אחראית על סיוע מרחוק במחשב זה. קיים סיכוי שמנהל יקבל גישה למחשב אחר, אולם הוא לא יכול להתחבר למחשב של המשתמש ללא הודעה מוקדמת או לשלוט בו ללא אישור מהמשתמש. כאשר מנהל מנסה להתחבר, המשתמש עדיין יכול לבחור לסרב להתחברות או לתת למנהל הרשאות תצוגה בלבד. על המשתמש ללחוץ במפורש על כפתור "כן" כדי לאפשר למנהל לשלוט מרחוק בתחנת העבודה.
      19. ההגדרה Microsoft Support Diagnostic Tool: Turn on MSDT interactive communication with support provider מגדירה את התקשורת של כלי האבחון של Microsoft עם ספק התמיכה. מומלץ שלא לשלוח נתונים לצד שלישי מכיוון שנתונים אלה עלולים להכיל מידע רגיש.
      20. ההגדרה Turn off the advertising ID מכבה את מזהה הפרסום, ומונעת מאפליקציות להשתמש במזהה .
      21. ההגדרה Allow Microsoft accounts to be optional קובעת האם חשבונות Microsoft הינם אופציונליים עבור יישומי החנות שדורשים כניסה לחשבון. הפעלת הגדרה זו מאפשרת לארגון להשתמש בחשבונות המשתמש הארגוניים במקום להשתמש בחשבונות Microsoft בעת גישה לחנות האפליקציות.
      22. ההגדרה Block launching Windows Store apps with Windows Runtime API access from hosted content קובעת האם ניתן להפעיל יישומי Windows אוניברסליים עם גישה ל-Windows Runtime API ישירות מהאינטרנט.
      23. ההגדרה Use enhanced anti-spoofing when available קובעת אם מוגדר anti-spoofing עבור מכשירים התומכים בה.
      24. ההגדרה Allow Use of Camera קובעת האם ניתן להשתמש בהתקני מצלמה. מצלמות בסביבות אבטחה גבוהות עשויות להוות סיכונים חמורים בפרטיות המשתמש.
      25. ההגדרה Turn off Microsoft consumer experiences מכבה חוויות המסייעות לצרכנים להפיק את המירב ממכשיריהם ומחשבון Microsoft. האפליקציות מחזירות נתונים לצד שלישי ועל כן מהוות סיכון בהקשר של דליפת נתונים אישיים.
      26. ההגדרה Require pin for pairing מגדירה האם יתבצע שימוש בקוד PIN בעמדה.
      27. ההגדרה Turn off location מכבה את אפשרות המיקום במחשב. מנקודה של אבטחת מידע, לא מומלץ לחשוף לתוכנות את המיקום ממנו עובדים.
      28. ההגדרה Shutdown: Allow system to be shut down without having to log on קובעת אם ניתן לכבות מחשב כאשר משתמש אינו מחובר. אם הגדרת מדיניות זו מופעלת, פקודת הכיבוי זמינה במסך הכניסה של Windows. מומלץ להשבית את הגדרת המדיניות הזו כדי להגביל את האפשרות לכבות את המחשב למשתמשים עם אישורים במערכת.
      29. ההגדרה Turn off access to the Store מציינת אם להשתמש בשירות החנות למציאת יישום לפתיחת קובץ עם סוג קובץ או שיוך פרוטוקול שלא מוכר במערת.
      30. ההגדרה Configure Offer Remote Assistance מאפשרת להפעיל או לבטל סיוע מרחוק ללא הזמנה במחשב זה. אנשי התמיכה לא יוכלו להציע סיוע באופן יזום, אם כי הם עדיין יכולים לענות לבקשות לסיוע משתמשים.
      31. ההגדרה Enable/Disable PerfTrack מציינת אם להפעיל או להשבית מעקב אחר אירועי תגובה.
      32. ההגדרה Do not preserve zone information in file attachments מאפשרת לקבוע אם Windows תסמן קבצים מצורפים עם מידע על אזור המוצא שלהם, כגון: מוגבל, אינטרנט, אינטרא-נט, מקומי. הגדרה זו דורשת NTFS על מנת לתפקד כראוי והיא תכשל ללא הודעה מוקדמת ב-FAT32. בכך שאינה שומרת את פרטי האזור, Windows אינה יכולה לבצע הערכות סיכונים נכונות.
      33. ההגדרה Let Windows apps מאפשרת לאפליקציות Windows לגשת למידע במערכת כגון מידע בחשבון, היסטוריית שיחות, אנשי קשר, דואל אלקטרוני, מיקום, קריאה או שליחת הודעות טקסט, נתוני תנועה, התראות וכו.

המלצות לתיקון:

* מומלץ להגדיר את ה- prevent the usage of OneDrive for file storage ל- Enabled:  
  Computer Configuration\Policies\Administrative Templates\Windows Components\OneDrive\Prevent the usage of OneDrive for file storage
* מומלץ להגדיר את ההגדרה Do not allow passwords to be saved ל-Enabled בנתיב הבא: Computer Configuration\Policies\Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Connection Client\Do not allow passwords to be saved
* מומלץ להגדיר את ההגדרה Do not allow COM port redirection ל Enabled בנתיב הבא: Computer Configuration\Policies\Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Session Host\Device and Resource Redirection\Do not allow COM port redirection
* מומלץ להגדיר את ההגדרה Do not allow drive redirection ל Enabled בנתיב הבא: Computer Configuration\Policies\Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Session Host\Device and Resource Redirection\Do not allow drive redirection
* מומלץ להגדיר את ההגדרה Do not allow LPT port redirection ל Enabled בנתיב הבא: Computer Configuration\Policies\Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Session Host\Device and Resource Redirection\Do not allow LPT port redirection
* מומלץ להגדיר את ההגדרה Do not allow supported Plug and Play device redirection כ-Enabled בנתיב הבא:  
  Computer Configuration\Policies\Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Session Host\Device and Resource Redirection\Do not allow supported Plug and Play device
* מומלץ להגדיר את ה- Prevent downloading of enclosures ל-Enabled בנתיב הבא:  
  Computer Configuration\Policies\Administrative Templates\Windows Components\RSS Feeds\Prevent downloading of enclosures
* מומלץ להגדיר את ההגדרה Turn off KMS Client Online AVS Validation ל-Enabled:  
  Computer Configuration\Policies\Administrative Templates\Windows Components\Software Protection Platform\Turn off KMS Client Online AVS Validation
* מומלץ להגדיר את ההגדרה Join Microsoft MAPS כ-Disabled:  
  Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Defender\MAPS\Join Microsoft MAPS
* מומלץ להגדיר את ההגדרה Configure Watson Events ל-Disabled:  
  Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Defender\Reporting\Configure Watson events
* מומלץ להגדיר את ההגדרות הקשורות ל- Windows Ink Workspace כ-Disabled:  
  Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Ink Workspace\Allow Windows Ink Workspace
* מומלץ להגדיר את ההגדרה Prevent users from sharing files within their profile כ-Enabled:  
  User Configuration\Policies\Administrative Templates\Windows Components\Network Sharing\Prevent users from sharing files within their profile.
* מומלץ להגדיר את ההגדרה Prevent Codec Download כ-Enabled:  
  User Configuration\Policies\Administrative Templates\Windows Components\Windows Media Player\Playback\Prevent Codec Download
* מומלץ להגדיר את ההגדרה Turn off multicast name resolution כ-Enabled בנתיב הבא:  
  Computer Configuration\Policies\Administrative Templates\Network\DNS Client\Turn off multicast name resolution
* מומלץ להגדיר את ההגדרה Enable Font Providers כ-Disabled:  
  Computer Configuration\Policies\Administrative Templates\Network\Fonts\Enable Font Providers
* מומלץ להגדיר את ההגדרה Untrusted Font Blocking כ- Enabled: Block untrusted fonts and log events בנתיב הבא:  
  Computer Configuration\Policies\Administrative Templates\System\Mitigation Options\Untrusted Font Blocking
* מומלץ להגדיר את ההגדרה Enable insecure guest logons כ-Disabled:  
  Computer Configuration\Policies\Administrative Templates\Network\Lanman Workstation\Enable insecure guest logons
* מומלץ להגדיר את ההגדרה Turn on Mapper I/O (LLTDIO) driver כ-Disabled:  
  Computer Configuration\Policies\Administrative Templates\Network\Link-Layer Topology Discovery\Turn on Mapper I/O (LLTDIO) driver
* מומלץ להגדיר את ההגדרה Turn on Responder (RSPNDR) driver כ-Disabled:  
  Computer Configuration\Policies\Administrative Templates\Network\Link-Layer Topology Discovery\Turn on Responder (RSPNDR) driver
* מומלץ להגדיר את ההגדרה Turn off Microsoft Peer-to-Peer Networking Services ל- Enabled בנתיב הבא:

Computer Configuration\Policies\Administrative Templates\Network\Microsoft Peer-to-Peer Networking Services\Turn off Microsoft Peer-to-Peer Networking Services

* מומלץ להגדיר את ההגדה Continue experiences on this device כ-Disabled:  
  Computer Configuration\Policies\Administrative Templates\System\Group Policy\Continue experiences on this device
* מומלץ להגדיר את ההגדרה Turn off background refresh of Group Policy כ-Disabled:  
  Computer Configuration\Policies\Administrative Templates\System\Group Policy\Turn off background refresh of Group Policy
* מומלץ להגדיר את ההגדרה Support device authentication using certificate כ-Enabled: Automatic:  
  Computer Configuration\Policies\Administrative Templates\System\Kerberos\Support device authentication using certificate
* מומלץ להגדיר את ההגדרה Disallow copying of user input methods to the system account for sign-in כ-Enabled:  
  Computer Configuration\Policies\Administrative Templates\System\Locale Services\Disallow copying of user input methods to the system account for sign-in
* מומלץ להגדיר את ההגדרה Configure Solicited Remote Assistance כ-Disabled בנתיב הבא:  
  Computer Configuration\Policies\Administrative Templates\System\Remote Assistance\Configure Solicited Remote Assistance
* מומלץ להגדיר את ההגדרה Microsoft Support Diagnostic Tool: Turn on MSDT interactive communication with support provider כ-Disabled בנתיב הבא:  
  Computer Configuration\Policies\Administrative Templates\System\Troubleshooting and Diagnostics\Microsoft Support Diagnostic Tool\Microsoft Support Diagnostic Tool: Turn on MSDT interactive communication with support provider
* מומלץ להגדיר את ההגדרה Turn off the advertising ID כ-Enabled בנתיב הבא:  
  Computer Configuration\Policies\Administrative Templates\System\User Profiles\Turn off the advertising ID
* מומלץ להגדיר את ההגדרה Allow Microsoft accounts to be optional כ-Enabled בנתיב הבא:  
  Computer Configuration\Policies\Administrative Templates\Windows Components\App runtime\Allow Microsoft accounts to be optional
* מומלץ להגדיר את ההגדרה Block launching Windows Store apps with Windows Runtime API access from hosted content ל-Enabled בנתיב הבא:  
  Computer Configuration\Policies\Administrative Templates\Windows Components\App runtime\Block launching Windows Store apps with Windows Runtime API access from
* מומלץ להגדיר את ההגדרה Use enhanced anti-spoofing when available כ-Enabled בנתיב הבא:  
  Computer Configuration\Policies\Administrative Templates\Windows Components\Biometrics\Facial Features\Use enhanced anti-spoofing when available
* מומלץ להגדיר את ההגדרה Allow Use of Camera כ-Disabled בנתיב הבא:  
  Computer Configuration\Policies\Administrative Templates\Windows Components\Camera\Allow Use of Camera
* מומלץ להגדיר את ההגדרה Turn off Microsoft consumer experiences כ-Enabled בנתיב הבא:  
  Computer Configuration\Policies\Administrative Templates\Windows Components\Cloud Content\Turn off Microsoft consumer experiences
* מומלץ להגדיר את ההגדרה Require pin for pairing ל-Enabled בנתיב הבא:  
  Computer Configuration\Policies\Administrative Templates\Windows Components\Connect\Require pin for pairing
* מומלץ להגדיר את ההגדרה Turn off location כ-Enabled בנתיב הבא:  
  Computer Configuration\Policies\Administrative Templates\Windows Components\Location and Sensors\Turn off location
* מומלץ להגדיר את ההגדרה Shutdown: Allow system to be shut down without having to log on ל-Disabled בנתיב הבא:  
  Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Shutdown: Allow system to be shut down without having to log on
* מומלץ להגדיר את ההגדרה Turn off access to the Store ב-Enabled בנתיב הבא:  
  Computer Configuration\Policies\Administrative Templates\System\Internet Communication Management\Internet Communication settings\Turn off access to the Store
* מומלץ להגדיר את ההגדרה Configure Offer Remote Assistance ל-Disabled בנתיב הבא:  
  Computer Configuration\Policies\Administrative Templates\System\Remote Assistance\Configure Offer Remote Assistance
* מומלץ להגדיר את ההגדרה Enable/Disable PerfTrack ל-Disabled בנתיב הבא:  
  Computer Configuration\Policies\Administrative Templates\System\Troubleshooting and Diagnostics\Windows Performance PerfTrack\Enable/Disable PerfTrack
* מומלץ להגדיר את ההגדרה Do not preserve zone information in file attachments כ-Disabled בנתיב הבא:  
  User Configuration\Policies\Administrative Templates\Windows Components\Attachment Manager\Do not preserve zone information in file attachments
* מומלץ להגדיר את כל ההגדרות הקשורות ל-Let Windows apps ל-Force Deny בנתיב הבא:  
  HKLM\Software\Policies\Microsoft\Winodws\AppPrivacy