09 נובמבר 2022
ט"ו חשון תשפ"ג
[עדכון]
10 נובמבר 2022
ט"ז חשון תשפ"ג
סימוכין:ב-ס-1507B

[עדכון] עדכון האבטחה החודשי של מיקרוסופט – נובמבר 2022

תקציר

ב-8 לחודש פרסמה מיקרוסופט כ-68 עדכוני אבטחה לפגיעויות בתוכנות נתמכות.

10 פגיעויות מסווגות בקריטיות.

6 פגיעויות מנוצלות בפועל על ידי תוקפים בעולם (Zero Day).

פורסם מידע פומבי לגבי 2 פגיעויות.

20 פגיעויות ניתנות לניצול על ידי תוקף מרוחק להרצת קוד (RCE).

מומלץ מאד לבחון העדכונים בסביבת ניסוי, ולהתקינם בהקדם האפשרי.

פרטים

1. המוצרים להם פורסמו עדכוני אבטחה הם:

- .NET Framework
- AMD CPU Branch
- Azure
- Azure Real Time Operating System
- Linux Kernel
- Microsoft Dynamics
- Microsoft Exchange Server
- Microsoft Graphics Component
- Microsoft Office
- Microsoft Office Excel
- Microsoft Office SharePoint
- Microsoft Office Word

- Network Policy Server (NPS)
- Open Source Software
- Role: Windows Hyper-V
- SysInternals
- Visual Studio
- Windows Advanced Local Procedure Call
- Windows ALPC
- Windows Bind Filter Driver
- Windows BitLocker
- Windows CNG Key Isolation Service
- Windows Devices Human Interface
- Windows Digital Media
- Windows DWM Core Library
- Windows Extensible File Allocation
- Windows Group Policy Preference Client
- Windows HTTP.sys
- Windows Kerberos
- Windows Mark of the Web (MOTW)
- Windows Netlogon
- Windows Network Address Translation (NAT)
- Windows ODBC Driver
- Windows Overlay Filter
- Windows Point-to-Point Tunneling Protocol
- Windows Print Spooler Components
- Windows Resilient File System (ReFS)
- Windows Scripting
- Windows Win32K

2. **תשומת לב כי לחלק מן העדכונים בקישור** https://msrc.microsoft.com/update-guide/releaseNote/2022-Nov **קיימת הפניה לפרטים נוספים וחלקם עשויים לדרוש ביצוע פעולות נוספות מעבר להתקנת העדכון עצמו. כמו כן הקישור מכיל מידע לגבי בעיות מוכרות בעדכוני אבטחה אלו.**
3. פירוט כלל העדכונים לחודש זה ניתן למצוא בקישור https://isc.sans.edu/diary/Microsoft+November+2022+Patch+Tuesday/29230.
4. **אם אינכם מתקינים עדכון אבטחה מצטבר (Cumulative) אלא בוחרים פרטנית אילו עדכונים להטמיע, מומלץ לתעדף את בדיקת והתקנת העדכונים המסומנים כקריטיים בקישור הנ"ל, או**

מסומנים כ-"More Likely" תחת העמודה Exploitability, או מאפשרים הרצת קוד מרחוק (Remote Code Execution), או מנוצלים בפועל על ידי תוקפים (Zero Day).

5. **מומלץ לתעדף בחינת והתקנת העדכונים לפגיעויות הבאות:**

1. 2 פגיעויות בשרתי Exchange (מוכרות כ-ProxyNotShell), שדווחו בהתרעת המערך של חודש אוקטובר אך לא היה עבורן עדכון אבטחה. פגיעויות אלו מנוצלות בפועל על ידי תוקפים בעולם, ולמרות שהחברה פרסמה הנחיות כיצד לנטרל הפגיעויות, היא ממליצה כעת להתקין את העדכונים ולא להסתמך על מעקפים אלו. קיימת פגיעות נוספת בשרתים אלו העלולה לאפשר לתוקף העלאת הרשאות, ולפי הפרסום צפויה להיות מנוצלת בפועל על ידי תוקפים.
2. פגיעות שפורסמה ומנוצלת בפועל על ידי תוקפים, במנגנון האבטחה המוכר כ-MOTW (Mark of the Web), המשמש להגנה מקבצים המורדים מרשת האינטרנט. פגיעות נוספת ברכיב זה תוקנה גם היא.
3. פגיעות מנוצלת בפועל בשרתי הדפסה (Print Spooler) עלולה לאפשר העלאת הרשאות.
4. פגיעות מנוצלת בפועל במנגנון ה-Scripting של מערכת ההפעלה עלולה לאפשר הרצת קוד מרחוק. ניצול הפגיעות אפשרי על ידי הכוונת המשתמש לשרת (Web או Share) זדוני. קיימת פגיעות קריטית נוספת בשירות זה.
5. פגיעות מנוצלת בפועל במנגנון ההגנה על מפתחות הצפנה פרטיים (Windows CNG Key Isolation Service) עלולה לאפשר העלאת הרשאות.
6. 2 פגיעויות בשרתי SharePoint עלולות לאפשר הרצת קוד מרחוק.
7. 2 פגיעויות בתוכנת אקסל עלולות לאפשר הרצת קוד מרחוק.
8. פגיעות בתוכנת Word עלולה לאפשר הרצת קוד מרחוק.
9. פגיעות בשירות Sysmon עלולה לאפשר לתוקף מקומי העלאת הרשאות לרמת System.
10. [עדכון] פגיעות בשירות Netlogon עלולה לאפשר לתוקף מרוחק העלאת הרשאות לרמת מנהלן. הטיפול בפגיעות זו כולל מספר שלבים. מומלץ לקרוא היטב את הפרטים בפרסומי החברה, ולבחון השינויים בסביבת ניסוי טרם הטמעה בסביבת ייצור:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-38023

- https://support.microsoft.com/en-us/topic/kb5021130-how-to-manage-the-netlogon-protocol-changes-related-to-cve-2022-38023-46ea3067-3989-4d40-963c-680fd9e8ee25

11. [עדכון] 2 פגיעויות קריטיות בשירות Kerberos עלולות לאפשר העלאת הרשאות. הטיפול בפגיעות זו כולל מספר שלבים. מומלץ לקרוא היטב את הפרטים בפרסומי החברה, ולבחון השינויים בסביבת ניסוי טרם הטמעה בסביבת ייצור:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-37966
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-37967
- https://support.microsoft.com/en-us/topic/kb5021131-how-to-manage-the-kerberos-protocol-changes-related-to-cve-2022-37966-fd837ac3-cdec-4e76-a6ec-86e67501407d
- https://support.microsoft.com/en-us/topic/kb5020805-how-to-manage-kerberos-protocol-changes-related-to-cve-2022-37967-997e9acc-67c5-48e1-8d0d-190269bf4efb

12. פגיעות קריטית ב-Github עלולה לאפשר הזרקת קוד ב-Azure CLI.

13. פגיעות קריטית ב-Hyper-V עלולה לאפשר מתקפת מניעת שירות.

14. 3 פגיעויות (מתוכן 2 קריטיות) בשירות PPTP עלולות לאפשר הרצת קוד מרחוק.

15. **20 פגיעויות ברכיבים/תוכנות הבאות עלולות לאפשר הרצת קוד מרחוק:**

1. CVE-2022-41051 Azure RTOS GUIX Studio Remote Code Execution Vulnerability
2. CVE-2022-41082 Microsoft Exchange Server Remote Code Execution Vulnerability
3. CVE-2022-41052 Windows Graphics Component Remote Code Execution Vulnerability
4. CVE-2022-41107 Microsoft Office Graphics Remote Code Execution Vulnerability
5. CVE-2022-41106 Microsoft Excel Remote Code Execution Vulnerability
6. CVE-2022-41063 Microsoft Excel Remote Code Execution Vulnerability
7. CVE-2022-41062 Microsoft SharePoint Server Remote Code Execution Vulnerability
8. CVE-2022-35823 Microsoft SharePoint Remote Code Execution Vulnerability

9. CVE-2022-41061 Microsoft Word Remote Code Execution Vulnerability
10. CVE-2022-41119 Visual Studio Remote Code Execution Vulnerability
11. CVE-2022-41048 Microsoft ODBC Driver Remote Code Execution Vulnerability
12. CVE-2022-41047 Microsoft ODBC Driver Remote Code Execution Vulnerability
13. CVE-2022-34734 Microsoft ODBC Driver Remote Code Execution Vulnerability
14. CVE-2022-34732 Microsoft ODBC Driver Remote Code Execution Vulnerability
15. CVE-2022-34730 Microsoft ODBC Driver Remote Code Execution Vulnerability
16. CVE-2022-41088 Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability
17. CVE-2022-41044 Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability
18. CVE-2022-41039 Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability
19. CVE-2022-41128 Windows Scripting Languages Remote Code Execution Vulnerability
20. CVE-2022-41118 Windows Scripting Languages Remote Code Execution Vulnerability

16. **31 פגיעויות ברכיבים/תוכנות הבאות עלולות לאפשר העלאת הרשאות:**

1. CVE-2022-41085 Azure CycleCloud Elevation of Privilege Vulnerability
2. CVE-2022-38014 Windows Subsystem for Linux (WSL2) Kernel Elevation of Privilege Vulnerability
3. CVE-2022-41123 Microsoft Exchange Server Elevation of Privilege Vulnerability
4. CVE-2022-41080 Microsoft Exchange Server Elevation of Privilege Vulnerability
5. CVE-2022-41040 Microsoft Exchange Server Elevation of Privilege Vulnerability
6. CVE-2022-41113 Windows Win32 Kernel Subsystem Elevation of Privilege Vulnerability
7. CVE-2022-41120 Microsoft Windows Sysmon Elevation of Privilege Vulnerability

8. CVE-2022-41093 Windows Advanced Local Procedure Call (ALPC) Elevation of Privilege Vulnerability
9. CVE-2022-41100 Windows Advanced Local Procedure Call (ALPC) Elevation of Privilege Vulnerability
10. CVE-2022-41045 Windows Advanced Local Procedure Call (ALPC) Elevation of Privilege Vulnerability
11. CVE-2022-41114 Windows Bind Filter Driver Elevation of Privilege Vulnerability
12. CVE-2022-41125 Windows CNG Key Isolation Service Elevation of Privilege Vulnerability
13. CVE-2022-41095 Windows Digital Media Receiver Elevation of Privilege Vulnerability
14. CVE-2022-41096 Microsoft DWM Core Library Elevation of Privilege Vulnerability
15. CVE-2022-41050 Windows Extensible File Allocation Table Elevation of Privilege Vulnerability
16. CVE-2022-37975 Windows Group Policy Elevation of Privilege Vulnerability
17. CVE-2022-41086 Windows Group Policy Elevation of Privilege Vulnerability
18. CVE-2022-37992 Windows Group Policy Elevation of Privilege Vulnerability
19. CVE-2022-41057 Windows HTTP.sys Elevation of Privilege Vulnerability
20. CVE-2022-37967 Windows Kerberos Elevation of Privilege Vulnerability
21. CVE-2022-37966 Windows Kerberos RC4-HMAC Elevation of Privilege Vulnerability
22. CVE-2022-38022 Windows Kernel Elevation of Privilege Vulnerability
23. CVE-2022-38023 Netlogon RPC Elevation of Privilege Vulnerability
24. CVE-2022-41102 Windows Overlay Filter Elevation of Privilege Vulnerability
25. CVE-2022-41101 Windows Overlay Filter Elevation of Privilege Vulnerability
26. CVE-2022-41073 Windows Print Spooler Elevation of Privilege Vulnerability
27. CVE-2022-41054 Windows Resilient File System (ReFS) Elevation of Privilege Vulnerability
28. CVE-2022-38045 Windows Server Service Elevation of Privilege Vulnerability

29. CVE-2022-41109 Windows Win32k Elevation of Privilege Vulnerability
30. CVE-2022-41092 Windows Win32k Elevation of Privilege Vulnerability
31. CVE-2022-38034 Windows Workstation Service Elevation of Privilege Vulnerability

17. 7 פגיעויות ברכיבים/תוכנות הבאות עלולות לאפשר מתקפת מניעת שירות:

1. CVE-2022-41056 Network Policy Server (NPS) RADIUS Protocol Denial of Service Vulnerability
2. CVE-2022-38015 Windows Hyper-V Denial of Service Vulnerability
3. CVE-2022-41053 Windows Kerberos Denial of Service Vulnerability
4. CVE-2022-37973 Windows Local Session Manager (LSM) Denial of Service Vulnerability
5. CVE-2022-41058 Windows Network Address Translation (NAT) Denial of Service Vulnerability
6. CVE-2022-41116 Windows Point-to-Point Tunneling Protocol Denial of Service Vulnerability
7. CVE-2022-41090 Windows Point-to-Point Tunneling Protocol Denial of Service Vulnerability

18. 4 פגיעויות ברכיבים/תוכנות הבאות עלולה לאפשר מעקף של אמצעי אבטחה

1. CVE-2022-41104 Microsoft Excel Security Feature Bypass Vulnerability
2. CVE-2022-41099 BitLocker Security Feature Bypass Vulnerability
3. CVE-2022-41091 Windows Mark of the Web Security Feature Bypass Vulnerability
4. CVE-2022-41049 Windows Mark of the Web Security Feature Bypass Vulnerability

דרכי התמודדות

1. משתמשים פרטיים עם מערכות נתמכות - מומלץ להשתמש בהקדם האפשרי בממשק העדכון האוטומטי של מערכת ההפעלה על מנת לעדכן את מערכותיכם ("בדוק אם קיימים עדכונים", בממשק הניהול).

2. משתמשים ארגוניים - מומלץ לבחון בסביבת ניסוי את התאמת העדכונים למערכותיכם, ולהתקינם בהקדם האפשרי.

3. מצורף קובץ Excel עם פירוט הפגיעויות בחלוקה למשפחות מוצרים. מקור - אתר העדכונים של מיקרוסופט.

שיתוף מידע עם ה-CERT הלאומי אינו מחליף חובת דיווח לגוף מנחה כלשהו, ככל שחלה על הגוף חובה כזו.
המידע נמסר כפי שהוא (as is), השימוש בו הוא באחריות המשתמש ומומלץ להיעזר באיש מקצוע בעל הכשרה מתאימה לצורך הטמעתו.