עדכון האבטחה החודשי של מיקרוסופט
מרץ 2026

12/03/2026
כ"ג אדר תשפ"ו

[תקציר]

- ב-10 לחודש פרסמה מיקרוסופט כ-87 עדכוני אבטחה לפגיעויות בתוכנות נתמכות.
- 0 פגיעויות מנוצלות בעולם על ידי תוקפים (Zero Day).
- פרטיהן של 2 פגיעויות פורסמו בפומבי.
- 3 פגיעויות מסווגות כקריטיות.
- 6 פגיעויות בעלות סיכוי גבוה לניצול בידי תוקפים.
- 20 פגיעויות ניתנות לניצול על ידי תוקף להרצת קוד מרחוק (RCE).
- מומלץ מאד לבחון העדכונים בסביבת ניסוי, ולהתקינם בהקדם האפשרי.

פעולות מידיות לביצוע:

- בחינה והתקנה בהקדם האפשרי של העדכונים שפרסמה החברה.
- לקוחות פרטיים – מומלץ לעדכן באמצעות מנגנון העדכון המובנה במערכת ההפעלה.
- ארגונים – מומלץ לבחון ולהתקין העדכונים בהקדם האפשרי.

[פרטים]

- את רשימת המוצרים להם פורסמו עדכוני אבטחה ניתן למצוא בקישור https://msrc.microsoft.com/update-guide/releaseNote/2026-Mar. תשומת לב כי לחלק מן העדכונים בקישור זה 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.
- פירוט כלל העדכונים לחודש זה ניתן למצוא בקישור https://isc.sans.edu/diary/Microsoft+Patch+Tuesday+March+2026/32782.
- 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).

1. **מומלץ לתעדף בחינת והתקנת העדכונים לפגיעויות הבאות:**
    1. פגיעויות ברכיבים הבאים, שפרטיהן פורסמו בפומבי:
        - .NET (הפגיעות עלולה לאפשר מתקפת מניעת שירות)
        - SQL Server (הפגיעות עלולה לאפשר העלאת הרשאות)
    2. פגיעויות קריטיות ברכיבים הבאים:
        - Microsoft Office
        - Microsoft Excel
    3. פגיעויות בעלות סיכוי גבוה להיות מנוצלות בידי תוקפים, ברכיבים הבאים:
        - Microsoft Graphics Component
        - Windows Accessibility Infrastructure (ATBroker.exe)
        - Windows Kernel
        - Windows SMB Server
        - Winlogon
    4. פגיעות בשירות Active Directory Domain Services עלולה לאפשר העלאת הרשאות.
    5. 6 פגיעויות ברכיב Active Directory Domain Services עלולות לאפשר דלף מידע או התחזות.
    6. 4 פגיעויות ברכיב Microsoft Graphics Component עלולות לאפשר העלאת הרשאות, מתקפת מניעת שירות או התחזות.
    7. 4 פגיעויות בתוכנת Office עלולות לאפשר הרצת קוד מרחוק או העלאת הרשאות.
    8. 5 פגיעויות בתוכנת Excel עלולות לאפשר הרצת קוד מרחוק או דלף מידע.
    9. 3 פגיעויות בתוכנת SharePoint עלולות לאפשר הרצת קוד מרחוק או התחזות.
    10. פגיעות בשירות Hyper-V עלולה לאפשר העלאת הרשאות.
    11. 3 פגיעויות בשרת SQL Server עלולות לאפשר העלאת הרשאות.
    12. 4 פגיעויות ברכיב Windows Ancillary Function Driver for WinSock עלולות לאפשר העלאת הרשאות.

2.13 פגיעויות ברכיב Windows Bluetooth RFCOM Protocol Driver עלולות לאפשר העלאת הרשאות.

3.14 פגיעויות ברכיב Windows Device Association Service עלולותת לאפשר העלאת הרשאות.

15. פגיעות בשירות Kerberos עלולה לאפשר מעקף שח אמצעי אבטחה.

3.16 פגיעויות ב-Kernel עלולות לאפשר העלאת הרשאות.

17. פגיעות ברכיב Windows GDI עלולה לאפשר הרצת קוד מרחוק.

18. פגיעות בשירות Windows NTFS עלולה לאפשר העלאת הרשאות.

6.19 פגיעויות בשירות Windows Routing and Remote Access Service (RRAS) עלולות לאפשר הרצת קוד מרחוק.

2.20 פגיעויות בשרת SMB עלולות לאפשר העלאת הרשאות.

21. פגיעות ברכיב Windows Win32K עלולה לאפשר העלאת הרשאות.

22. פגיעות בשירות Winlogon עלולה לאפשר העלאת הרשאות.

23. פגיעות ברכיב Azure MCP עלולה לאפשר העלאת הרשאות.

24. פגיעות בשירות Windows Print Spooler עלולה לאפשר הרצת קוד מרחוק.

25. **20 פגיעויות ברכיבים/תוכנות הבאות עלולות לאפשר הרצת קוד מרחוק:**

1. CVE-2026-23654 GitHub: Zero Shot SCFoundation Remote Code Execution Vulnerability
2. CVE-2026-26113 Microsoft Office Remote Code Execution Vulnerability
3. CVE-2026-26110 Microsoft Office Remote Code Execution Vulnerability
4. CVE-2026-26107 Microsoft Excel Remote Code Execution Vulnerability
5. CVE-2026-26112 Microsoft Excel Remote Code Execution Vulnerability
6. CVE-2026-26109 Microsoft Excel Remote Code Execution Vulnerability
7. CVE-2026-26108 Microsoft Excel Remote Code Execution Vulnerability
8. CVE-2026-26114 Microsoft SharePoint Server Remote Code Execution Vulnerability
9. CVE-2026-26106 Microsoft SharePoint Server Remote Code Execution Vulnerability

10. CVE-2026-26030 GitHub: CVE-2026-26030 Microsoft Semantic Kernel InMemoryVectorStore filter functionality vulnerable
11. CVE-2026-25190 GDI Remote Code Execution Vulnerability
12. CVE-2026-24288 Windows Mobile Broadband Driver Remote Code Execution Vulnerability
13. CVE-2026-23669 Windows Print Spooler Remote Code Execution Vulnerability
14. CVE-2026-25172 Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability
15. CVE-2026-25172 Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability
16. CVE-2026-25173 Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability
17. CVE-2026-25173 Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability
18. CVE-2026-26111 Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability
19. CVE-2026-26111 Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability
20. CVE-2026-25166 Windows System Image Manager Assessment and Deployment Kit (ADK) Remote Code Execution Vulnerability

26. 46 פגיעויות ברכיבים/תוכנות הבאות עלולות לאפשר העלאת הרשאות:

1. CVE-2026-26131 .NET Elevation of Privilege Vulnerability
2. CVE-2026-25177 Active Directory Domain Services Elevation of Privilege Vulnerability
3. CVE-2026-26141 Hybrid Worker Extension (Arc-enabled Windows VMs) Elevation of Privilege Vulnerability
4. CVE-2026-26148 Microsoft Azure AD SSH Login extension for Linux Elevation of Privilege Vulnerability

5. CVE-2026-23665 Linux Azure Diagnostic extension (LAD) Elevation of Privilege Vulnerability
6. CVE-2026-26118 Azure MCP Server Tools Elevation of Privilege Vulnerability
7. CVE-2026-23660 Windows Admin Center in Azure Portal Elevation of Privilege Vulnerability
8. CVE-2026-26117 Arc Enabled Servers - Azure Connected Machine Agent Elevation of Privilege Vulnerability
9. CVE-2026-23667 Broadcast DVR Elevation of Privilege Vulnerability
10. CVE-2026-24292 Windows Connected Devices Platform Service Elevation of Privilege Vulnerability
11. CVE-2026-25167 Microsoft Brokering File System Elevation of Privilege Vulnerability
12. CVE-2026-23668 Windows Graphics Component Elevation of Privilege Vulnerability
13. CVE-2026-26134 Microsoft Office Elevation of Privilege Vulnerability
14. CVE-2026-26134 Microsoft Office Elevation of Privilege Vulnerability
15. CVE-2026-25170 Windows Hyper-V Elevation of Privilege Vulnerability
16. CVE-2026-26116 SQL Server Elevation of Privilege Vulnerability
17. CVE-2026-26115 SQL Server Elevation of Privilege Vulnerability
18. CVE-2026-21262 SQL Server Elevation of Privilege Vulnerability
19. CVE-2026-20967 System Center Operations Manager (SCOM) Elevation of Privilege Vulnerability
20. CVE-2026-24291 Windows Accessibility Infrastructure (ATBroker.exe) Elevation of Privilege Vulnerability
21. CVE-2026-25179 Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability
22. CVE-2026-25176 Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability

23. CVE-2026-24293 Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability
24. CVE-2026-25178 Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability
25. CVE-2026-25171 Windows Authentication Elevation of Privilege Vulnerability
26. CVE-2026-23671 Windows Bluetooth RFCOM Protocol Driver Elevation of Privilege Vulnerability
27. CVE-2026-23671 Windows Bluetooth RFCOM Protocol Driver Elevation of Privilege Vulnerability
28. CVE-2026-24296 Windows Device Association Service Elevation of Privilege Vulnerability
29. CVE-2026-24295 Windows Device Association Service Elevation of Privilege Vulnerability
30. CVE-2026-24295 Windows Device Association Service Elevation of Privilege Vulnerability
31. CVE-2026-25189 Windows DWM Core Library Elevation of Privilege Vulnerability
32. CVE-2026-25174 Windows Extensible File Allocation Table Elevation of Privilege Vulnerability
33. CVE-2026-24283 Multiple UNC Provider Kernel Driver Elevation of Privilege Vulnerability
34. CVE-2026-24289 Windows Kernel Elevation of Privilege Vulnerability
35. CVE-2026-26132 Windows Kernel Elevation of Privilege Vulnerability
36. CVE-2026-24287 Windows Kernel Elevation of Privilege Vulnerability
37. CVE-2026-25175 Windows NTFS Elevation of Privilege Vulnerability
38. CVE-2026-25165 Performance Counters for Windows Elevation of Privilege Vulnerability

39. CVE-2026-24290 Windows Projected File System Elevation of Privilege Vulnerability
40. CVE-2026-23673 Windows Resilient File System (ReFS) Elevation of Privilege Vulnerability
41. CVE-2026-26128 Windows SMB Server Elevation of Privilege Vulnerability
42. CVE-2026-24294 Windows SMB Server Elevation of Privilege Vulnerability
43. CVE-2026-25188 Windows Telephony Service Elevation of Privilege Vulnerability
44. CVE-2026-23672 Windows Universal Disk Format File System Driver (UDFS) Elevation of Privilege Vulnerability
45. CVE-2026-24285 Win32k Elevation of Privilege Vulnerability
46. CVE-2026-25187 Winlogon Elevation of Privilege Vulnerability

27. **4 פגיעויות ברכיבים/תוכנות הבאות עלולות לאפשר מתקפת מניעת שירות:**

1. CVE-2026-26127 .NET Denial of Service Vulnerability
2. CVE-2026-26130 ASP.NET Core Denial of Service Vulnerability
3. CVE-2026-25168 Windows Graphics Component Denial of Service Vulnerability
4. CVE-2026-25169 Windows Graphics Component Denial of Service Vulnerability

28. **2 פגיעויות ברכיבים/תוכנות הבאות עלולות לאפשר מעקף של מנגנון אבטחה:**

1. CVE-2026-24297 Windows Kerberos Security Feature Bypass Vulnerability
2. CVE-2026-23674 MapUrlToZone 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.

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