עדכון האבטחה החודשי של מיקרוסופט
אפריל 2026

17/04/2026
ל' ניסן תשפ"ו

[תקציר]

- ב-14 לחודש פרסמה מיקרוסופט כ-163 עדכוני אבטחה לפגיעויות בתוכנות נתמכות. בנוסף פורסמו 78 עדכוני אבטחה לדפדפן Edge המבוסס על מנוע Chromium.
- פגיעות אחת מנוצלת בעולם על ידי תוקפים (Zero Day).
- פרטיה של פגיעות אחת פורסמו בפומבי.
- 8 פגיעויות מסווגות כקריטיות (7 מתוכן עלולות לאפשר הרצת קוד מרחוק).
- 19 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-Apr. 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+April+2026/32898.
- 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:
      - Microsoft Defender
   2. פגיעויות קריטיות ברכיבים הבאים:
      - .NET Framework
      - Microsoft Office
      - Microsoft Office Word
      - Remote Desktop Client
      - Windows Active Directory
      - Windows IKE Extension
      - Windows TCP/IP
   3. פגיעויות בעלות סיכוי גבוה להיות מנוצלות בידי תוקפים, ברכיבים הבאים:
      - Desktop Window Manager
      - Function Discovery Service (fdwsd.dll)
      - Microsoft Defender
      - Microsoft Management Console
      - Microsoft Windows Search Component
      - Windows Active Directory
      - Windows BitLocker
      - Windows Boot Loader
      - Windows COM
      - Windows Common Log File System Driver
      - Windows Hello
      - Windows Kernel Memory
      - Windows Remote Desktop
      - Windows Shell
      - Windows TCP/IP
      - Windows TDI Translation Driver (tdx.sys)
      - Windows Universal Plug and Play (UPnP) Device Host
   4. פגיעות קריטית ב-Windows TCP/IP עלולה לאפשר לתוקף הרצת קוד מרחוק ללא צורך בהזדהות באמצעות משלוח IPv6 packet לציוד שמופעל בו שירות IPSec. **אם ארגונכם מפעיל שרת הנגיש באמצעות IPv6 מרשת האינטרנט**

ובנוסף מפעיל IPSec, מומלץ מאד לתעדף הטיפול בפגיעות זו מאחר ותיאורטית ניתן לנצל הפגיעות גם כתולעת (Wormable).

5. פגיעות ב-Microsoft Defender שפרטיה פורסמו בפומבי עלולה לאפשר העלאת הרשאות לרמת SYSTEM.
6. 2 פגיעויות בשרת Microsoft SharePoint עלולות לאפשר התחזות. אחת מהן מנוצלת בפועל על ידי תוקפים בעולם.
7. פגיעות קריטית ב-Windows Active Directory עלולה לאפשר הרצת קוד מרחוק באמצעות משלוח פניה בפרוטוקול RPC. התקיפה אפשרית מרשת סמוכה (adjacent).
8. פגיעות קריטית בתוכנת Office עלולה לאפשר הרצת קוד מרחוק. הפגיעות ניתנת לניצול באמצעות ה-Preview Pane.
9. 2 פגיעויות קריטיות בתוכנת Word עלולות לאפשר הרצת קוד מרחוק.
10. פגיעות בתוכנת הקליינט של RDP עלולה לאפשר לתוקף בעל אחיזה בשרת RDP, הרצת קוד מרחוק על עמדת המשתמש הניגש לשרת.
11. פגיעות קריטית בשירות Windows Internet Key Exchange (IKE) Service Extensions עלול לאפשר לתוקף הרצת קוד מרחוק על השרת. **כמעקף זמני עד להתקנת עדכון האבטחה**, ניתן להגביל הגישה לפורטים UDP/500,4500 לכתובות ספציפיות ומוכרות בלבד.
12. פגיעות קריטית ב-.NET Framework. עלולה לאפשר מתקפת מניעת שירות.
13. פגיעות ב-Windows Hello עלולה לאפשר מעקף של מנגנון ההזדהות.
14. פגיעות ב-Windows BitLocker עלולה לאפשר מעקף של מנגנון אבטחה.
15. 4 פגיעויות בתוכנת Excel עלולות לאפשר הרצת קוד מרחוק.
16. פגיעות ב-PowerShell עלולה לאפשר העלאת הרשאות. פגיעות נוספת עלולה לאפשר מעקף של אמצעי אבטחה.
17. 2 פגיעויות בשירות Hyper-V עלולות לאפשר הרצת קוד מרחוק.
18. פגיעות בשירות SQL Server עלולה לאפשר הרצת קוד מרחוק. 2 פגיעויות נוספות עלולות לאפשר העלאת הרשאות.
19. 8 פגיעויות ברכיב Windows Ancillary Function Driver for WinSock עלולות לאפשר העלאת הרשאות.

20. פגיעות ברכיב Windows HTTP.sys עלולה לאפשר מתקפת מניעת שירות.

21. פגיעות בשירות Windows Kerberos עלולה לאפשר העלאת הרשאות.

22. 4 פגיעויות ב-Windows Kernel עלולות לאפשר העלאת הרשאות.

23. פגיעות בתוכנה Windows Snipping Tool עלולה לאפשר הרצת קוד מרחוק.

24. 8 פגיעויות ברכיב Windows Universal Plug and Play (UPnP) Device Host עלולות לאפשר הרצת קוד מרחוק, העלאת הרשאות או דלף מידע.

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

1. CVE-2026-32221 Windows Graphics Component Remote Code Execution Vulnerability
2. CVE-2026-32190 Microsoft Office Remote Code Execution Vulnerability
3. CVE-2026-32199 Microsoft Excel Remote Code Execution Vulnerability
4. CVE-2026-32198 Microsoft Excel Remote Code Execution Vulnerability
5. CVE-2026-32197 Microsoft Excel Remote Code Execution Vulnerability
6. CVE-2026-32189 Microsoft Excel Remote Code Execution Vulnerability
7. CVE-2026-32200 Microsoft PowerPoint Remote Code Execution Vulnerability
8. CVE-2026-33115 Microsoft Word Remote Code Execution Vulnerability
9. CVE-2026-33114 Microsoft Word Remote Code Execution Vulnerability
10. CVE-2026-33095 Microsoft Word Remote Code Execution Vulnerability
11. CVE-2026-23657 Microsoft Word Remote Code Execution Vulnerability
12. CVE-2026-32157 Remote Desktop Client Remote Code Execution Vulnerability
13. CVE-2026-32149 Windows Hyper-V Remote Code Execution Vulnerability
14. CVE-2026-26156 Windows Hyper-V Remote Code Execution Vulnerability
15. CVE-2026-33120 Microsoft SQL Server Remote Code Execution Vulnerability
16. CVE-2026-33826 Windows Active Directory Remote Code Execution Vulnerability
17. CVE-2026-33824 Windows Internet Key Exchange (IKE) Service Extensions Remote Code Execution Vulnerability

18. CVE-2026-32183 Windows Snipping Tool Remote Code Execution Vulnerability
19. CVE-2026-33827 Windows TCP/IP Remote Code Execution Vulnerability
20. CVE-2026-32156 Windows UPnP Device Host Remote Code Execution Vulnerability

26. 93 פגיעויות ברכיבים/תוכנות הבאות עלולות לאפשר העלאת הרשאות:

1. CVE-2026-25184 Applocker Filter Driver (applockerfltr.sys) Elevation of Privilege Vulnerability
2. CVE-2026-32171 Azure Logic Apps Elevation of Privilege Vulnerability
3. CVE-2026-32192 Azure Monitor Agent Elevation of Privilege Vulnerability
4. CVE-2026-32168 Azure Monitor Agent Elevation of Privilege Vulnerability
5. CVE-2026-32155 Desktop Window Manager Elevation of Privilege Vulnerability
6. CVE-2026-32154 Desktop Window Manager Elevation of Privilege Vulnerability
7. CVE-2026-32152 Desktop Window Manager Elevation of Privilege Vulnerability
8. CVE-2026-27924 Desktop Window Manager Elevation of Privilege Vulnerability
9. CVE-2026-27923 Desktop Window Manager Elevation of Privilege Vulnerability
10. CVE-2026-32150 Windows Function Discovery Service (fdwsd.dll) Elevation of Privilege Vulnerability
11. CVE-2026-32093 Windows Function Discovery Service (fdwsd.dll) Elevation of Privilege Vulnerability
12. CVE-2026-32087 Windows Function Discovery Service (fdwsd.dll) Elevation of Privilege Vulnerability
13. CVE-2026-32086 Windows Function Discovery Service (fdwsd.dll) Elevation of Privilege Vulnerability

14. CVE-2026-32219 Microsoft Brokering File System Elevation of Privilege Vulnerability
15. CVE-2026-32091 Microsoft Brokering File System Elevation of Privilege Vulnerability
16. CVE-2026-26181 Microsoft Brokering File System Elevation of Privilege Vulnerability
17. CVE-2026-33825 Microsoft Defender Elevation of Privilege Vulnerability
18. CVE-2026-32184 Microsoft High Performance Compute (HPC) Pack Elevation of Privilege Vulnerability
19. CVE-2026-27914 Microsoft Management Console Elevation of Privilege Vulnerability
20. CVE-2026-26170 PowerShell Elevation of Privilege Vulnerability
21. CVE-2026-27909 Windows Search Service Elevation of Privilege Vulnerability
22. CVE-2026-32153 Windows Speech Runtime Elevation of Privilege Vulnerability
23. CVE-2026-32176 SQL Server Elevation of Privilege Vulnerability
24. CVE-2026-32167 SQL Server Elevation of Privilege Vulnerability
25. CVE-2026-26178 Windows Advanced Rasterization Platform Elevation of Privilege Vulnerability
26. CVE-2026-33100 Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability
27. CVE-2026-33099 Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability
28. CVE-2026-32073 Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability
29. CVE-2026-27922 Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability

30. CVE-2026-26182 Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability
31. CVE-2026-26177 Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability
32. CVE-2026-26173 Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability
33. CVE-2026-26168 Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability
34. CVE-2026-26176 Windows Client Side Caching driver (csc.sys) Elevation of Privilege Vulnerability
35. CVE-2026-27926 Windows Cloud Files Mini Filter Driver Elevation of Privilege Vulnerability
36. CVE-2026-32162 Windows COM Elevation of Privilege Vulnerability
37. CVE-2026-32070 Windows Common Log File System Driver Elevation of Privilege Vulnerability
38. CVE-2026-33098 Windows Container Isolation FS Filter Driver Elevation of Privilege Vulnerability
39. CVE-2026-26152 Microsoft Cryptographic Services Elevation of Privilege Vulnerability
40. CVE-2026-26153 Windows Encrypted File System (EFS) Elevation of Privilege Vulnerability
41. CVE-2026-27910 Windows Installer Elevation of Privilege Vulnerability
42. CVE-2026-27912 Windows Kerberos Elevation of Privilege Vulnerability
43. CVE-2026-32195 Windows Kernel Elevation of Privilege Vulnerability
44. CVE-2026-26180 Windows Kernel Elevation of Privilege Vulnerability
45. CVE-2026-26179 Windows Kernel Elevation of Privilege Vulnerability
46. CVE-2026-26163 Windows Kernel Elevation of Privilege Vulnerability
47. CVE-2026-27929 Windows LUA File Virtualization Filter Driver Elevation of Privilege Vulnerability

48. CVE-2026-20930 Windows Management Services Elevation of Privilege Vulnerability
49. CVE-2026-26162 Windows OLE Elevation of Privilege Vulnerability
50. CVE-2026-33101 Windows Print Spooler Elevation of Privilege Vulnerability
51. CVE-2026-32078 Windows Projected File System Elevation of Privilege Vulnerability
52. CVE-2026-32074 Windows Projected File System Elevation of Privilege Vulnerability
53. CVE-2026-32069 Windows Projected File System Elevation of Privilege Vulnerability
54. CVE-2026-27927 Windows Projected File System Elevation of Privilege Vulnerability
55. CVE-2026-26184 Windows Projected File System Elevation of Privilege Vulnerability
56. CVE-2026-32160 Windows Push Notifications Elevation of Privilege Vulnerability
57. CVE-2026-32159 Windows Push Notifications Elevation of Privilege Vulnerability
58. CVE-2026-32158 Windows Push Notifications Elevation of Privilege Vulnerability
59. CVE-2026-26172 Windows Push Notifications Elevation of Privilege Vulnerability
60. CVE-2026-26167 Windows Push Notifications Elevation of Privilege Vulnerability
61. CVE-2026-26160 Remote Desktop Licensing Service Elevation of Privilege Vulnerability
62. CVE-2026-26159 Remote Desktop Licensing Service Elevation of Privilege Vulnerability

63. CVE-2026-26183 Remote Access Management service/API (RPC server) Elevation of Privilege Vulnerability
64. CVE-2026-26161 Windows Sensor Data Service Elevation of Privilege Vulnerability
65. CVE-2026-32224 Windows Server Update Service (WSUS) Elevation of Privilege Vulnerability
66. CVE-2026-26174 Windows Server Update Service (WSUS) Elevation of Privilege Vulnerability
67. CVE-2026-27918 Windows Shell Elevation of Privilege Vulnerability
68. CVE-2026-26166 Windows Shell Elevation of Privilege Vulnerability
69. CVE-2026-26165 Windows Shell Elevation of Privilege Vulnerability
70. CVE-2026-32090 Windows Speech Brokered Api Elevation of Privilege Vulnerability
71. CVE-2026-32089 Windows Speech Brokered Api Elevation of Privilege Vulnerability
72. CVE-2026-32083 Windows Simple Search and Discovery Protocol (SSDP) Service Elevation of Privilege Vulnerability
73. CVE-2026-32082 Windows Simple Search and Discovery Protocol (SSDP) Service Elevation of Privilege Vulnerability
74. CVE-2026-32068 Windows Simple Search and Discovery Protocol (SSDP) Service Elevation of Privilege Vulnerability
75. CVE-2026-32076 Windows Storage Spaces Controller Elevation of Privilege Vulnerability
76. CVE-2026-27907 Windows Storage Spaces Controller Elevation of Privilege Vulnerability
77. CVE-2026-27921 Windows TDI Translation Driver (tdx.sys) Elevation of Privilege Vulnerability
78. CVE-2026-27908 Windows TDI Translation Driver (tdx.sys) Elevation of Privilege Vulnerability

79. CVE-2026-32077 Windows UPnP Device Host Elevation of Privilege Vulnerability
80. CVE-2026-32075 Windows UPnP Device Host Elevation of Privilege Vulnerability
81. CVE-2026-27920 Windows UPnP Device Host Elevation of Privilege Vulnerability
82. CVE-2026-27919 Windows UPnP Device Host Elevation of Privilege Vulnerability
83. CVE-2026-27916 Windows UPnP Device Host Elevation of Privilege Vulnerability
84. CVE-2026-27915 Windows UPnP Device Host Elevation of Privilege Vulnerability
85. CVE-2026-32223 Windows USB Printing Stack (usbprint.sys) Elevation of Privilege Vulnerability
86. CVE-2026-32165 Windows User Interface Core Elevation of Privilege Vulnerability
87. CVE-2026-32164 Windows User Interface Core Elevation of Privilege Vulnerability
88. CVE-2026-32163 Windows User Interface Core Elevation of Privilege Vulnerability
89. CVE-2026-27911 Windows User Interface Core Elevation of Privilege Vulnerability
90. CVE-2026-32080 Windows WalletService Elevation of Privilege Vulnerability
91. CVE-2026-27917 Windows WFP NDIS Lightweight Filter Driver (wfplwfs.sys) Elevation of Privilege Vulnerability
92. CVE-2026-33104 Win32k Elevation of Privilege Vulnerability
93. CVE-2026-32222 Windows Win32k Elevation of Privilege Vulnerability

27. **9 פגיעויות ברכיבים/תוכנות הבאות עלולות לאפשר מתקפת מניעת שירות:**

1. CVE-2026-26171 .NET Denial of Service Vulnerability
2. CVE-2026-32203 .NET and Visual Studio Denial of Service Vulnerability
3. CVE-2026-32226 .NET Framework Denial of Service Vulnerability
4. CVE-2026-23666 .NET Framework Denial of Service Vulnerability
5. CVE-2026-33116 .NET, .NET Framework, and Visual Studio Denial of Service Vulnerability
6. CVE-2026-32181 Connected User Experiences and Telemetry Service Denial of Service Vulnerability
7. CVE-2026-33096 HTTP.sys Denial of Service Vulnerability
8. CVE-2026-32071 Windows Local Security Authority Subsystem Service (LSASS) Denial of Service Vulnerability
9. CVE-2026-32216 Windows Redirected Drive Buffering System Denial of Service Vulnerability

28. **12 פגיעויות ברכיבים/תוכנות הבאות עלולות לאפשר מעקף של מנגנון אבטחה:**

1. CVE-2026-26149 Microsoft Power Apps Security Feature Bypass
2. CVE-2026-26143 Microsoft PowerShell Security Feature Bypass Vulnerability
3. CVE-2026-32088 Windows Biometric Service Security Feature Bypass Vulnerability
4. CVE-2026-27913 Windows BitLocker Security Feature Bypass Vulnerability
5. CVE-2026-0390 UEFI Secure Boot Security Feature Bypass Vulnerability
6. CVE-2026-26175 Windows Boot Manager Security Feature Bypass Vulnerability
7. CVE-2026-27928 Windows Hello Security Feature Bypass Vulnerability
8. CVE-2026-27906 Windows Hello Security Feature Bypass Vulnerability
9. CVE-2026-20928 Windows Recovery Environment Security Feature Bypass Vulnerability
10. CVE-2026-32225 Windows Shell Security Feature Bypass Vulnerability

11. CVE-2026-32220 UEFI Secure Boot Security Feature Bypass Vulnerability
12. CVE-2026-23670 Windows Virtualization-Based Security (VBS) 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.