עדכון האבטחה החודשי של מיקרוסופט
יוני 2026

11/06/2026
כ"ו סיון תשפ"ו

[תקציר]

- ב-9 לחודש פרסמה מיקרוסופט כ-200 עדכוני אבטחה (עדכון האבטחה החודשי הגדול ביותר שפורסם על ידי החברה מעולם) לפגיעויות בתוכנות נתמכות. החברה גם עדכנה את דפדפן Edge המבוסס על Chromium במענה לכ-360 פגיעויות נוספות.
- פורסמו 13 עדכונים לפגיעויות שכבר פורסמו בעבר.
- פרטיהן של 3 פגיעויות פורסמו בפומבי. פגיעות אחת מנוצלת בפועל בעולם.
- 35 פגיעויות מסווגות כקריטיות (30 מתוכן עלולות לאפשר הרצת קוד מרחוק).
- 16 פגיעויות מוגדרות כבעלות סיכוי גבוה לניצול בידי תוקפים.
- 56 פגיעויות ניתנות לניצול על ידי תוקף להרצת קוד מרחוק (RCE).
- מומלץ מאד לבחון העדכונים בסביבת ניסוי, ולהתקינם בהקדם האפשרי.

[פרטים]

- את רשימת המוצרים להם פורסמו עדכוני אבטחה ניתן למצוא בקישור https://msrc.microsoft.com/update-guide/releaseNote/2026-Jun. 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+June+2026+Patch+Tuesday/33064/.
- 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).

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.

1. **מומלץ לתעדף בחינת והתקנת העדכונים לפגיעויות הבאות:**
   1. פגיעות קריטית בשרתי Exchange, שדווחה בחודש מאי 2025, ומנוצלת בפועל בעולם. לאחר פרסומה בחודש שעבר, הדרך המומלצת להתמודדות עם הפגיעות הייתה באמצעות Exchange Emergency Mitigation Service. כעת פורסם עדכון אבטחה לפגיעות זו. מומלץ לבוחנו ולהתקינו בהקדם האפשרי ולא להסתפק במענה באמצעות ה-Exchange Emergency Mitigation Service. לשרת Exchange פורסמו החודש עוד 7 פגיעויות שונות.
   2. פגיעויות קריטיות ברכיבים הבאים:
      - Active Directory Domain Services
      - Linux MANA Driver
      - Microsoft Azure Attestation service and Device Health Attestation Service
      - Microsoft Azure Kubernetes Service
      - Microsoft Exchange Server
      - Microsoft Office
      - Nuance PowerScribe
      - Remote Desktop Client
      - Role: Windows Hyper-V
      - Windows Cryptographic Services
      - Windows Deployment Services
      - Windows DHCP Client
      - Windows HTTP.sys
      - Windows Hyper-V
      - Windows Kerberos
      - Windows Kernel
      - Windows Media
      - Windows Remote Desktop
      - Windows Remote Desktop Services
      - Windows Win32K – GRFX

3. פגיעויות בעלות סיכוי גבוה להיות מנוצלות בידי תוקפים, ברכיבים הבאים:
   - HTTP/2
   - Microsoft Graphics Component
   - Microsoft Office SharePoint
   - Remote Desktop Client
   - Windows BitLocker
   - Windows Collaborative Translation Framework
   - Windows DWM Core Library
   - Windows HTTP.sys
   - Windows NT OS Kernel
   - Windows NTLM
   - Windows Win32K - GRFX
   - Winlogon
4. פגיעות בפרוטוקולים HTTP/2, HTTP/3 שפרטיה פורסמו בעולם, עלולה לאפשר בצורה קלה לניצול מתקפת מניעת שירות כנגד הרכיב HTTP.sys. פגיעות נוספת ברכיב זה מוגדרת כקריטית ועלולה לאפשר הרצת קוד מרחוק.
5. פגיעות ב-BitLocker שפרטיה פורסמו בפומבי, עלולה לאפשר מעקף של אמצעי אבטחה.
6. פגיעות ברכיב Windows Collaborative Translation Framework (CTFMON) שפרטיה פורסמו בפומבי, עלולה לאפשר העלאת הרשאות לרמת SYSTEM.
7. 8 פגיעויות קריטיות בתוכנת Office, 7 מתוכן עלולות לאפשר הרצת קוד מרחוק. בנוסף פורסמו עוד 6 פגיעויות בתוכנה זו.
8. 5 פגיעויות בתוכנת Word, 4 מתוכן עלולות לאפשר הרצת קוד מרחוק.
9. 8 פגיעויות בתוכנת Excel, 5 מתוכן עלולות לאפשר הרצת קוד מרחוק.
10. 21 פגיעויות בתוכנת SharePoint, 2 מתוכן עלולות לאפשר הרצת קוד מרחוק, כאשר עבור אחת מהן הרצת הקוד תתבצע אצל המשתמש המתחבר לשרת בשליטת תוקף.
11. 11 פגיעויות בתוכנה Remote Desktop Client עלולות לאפשר הרצת קוד מרחוק. 7 מהן מסווגות בקריטיות.
12. 3 פגיעויות קריטיות בשירות Hyper-V עלולות לאפשר הרצת קוד מרחוק.

13. 7 פגיעויות ברכיב Windows Ancillary Function Driver for WinSock עלולות לאפשר העלאת הרשאות.
14. פגיעות קריטית ב-Windows DHCP Client עלולה לאפשר הרצת קוד מרחוק.
15. 11 פגיעויות ברכיב Windows DWM Core Library. 9 מתוכן עלולות לאפשר העלאת הרשאות.
16. פגיעות קריטית ב-Windows Kerberos עלולה לאפשר הרצת קוד מרחוק בשרת Kerberos Key Distribution Center (KDC).
17. פגיעות קריטית ב-Kernel עלולה לאפשר הרצת קוד מרחוק.
18. פגיעות ב-NTFS עלולה לאפשר הרצת קוד מרחוק.
19. 8 פגיעויות ב-Windows Secure Boot, 7 מתוכן עלולות לאפשר מעקף של אמצעי אבטחה.
20. 2 פגיעויות ברכיב Windows Win32K – GRFX עלולות לאפשר הרצת קוד מרחוק.
21. פגיעות קריטית ב-Active Directory Domain Services עלולה לאפשר הרצת קוד מרחוק.
22. **56 פגיעויות ברכיבים/תוכנות הבאות עלולות לאפשר הרצת קוד מרחוק:**

1. CVE-2026-45648 Windows Active Directory Domain Services Remote Code Execution Vulnerability
2. CVE-2026-47643 Azure Stack Edge Remote Code Execution Vulnerability
3. CVE-2026-32193 Azure Kubernetes Service (AKS) Remote Code Execution Vulnerability
4. CVE-2026-45583 Microsoft Exchange Server Remote Code Execution Vulnerability
5. CVE-2026-47635 Microsoft Outlook and Word Remote Code Execution Vulnerability
6. CVE-2026-45645 Microsoft Office Remote Code Execution Vulnerability
7. CVE-2026-45475 Microsoft Office Remote Code Execution Vulnerability
8. CVE-2026-45474 Microsoft Office Remote Code Execution Vulnerability
9. CVE-2026-45472 Microsoft Office Remote Code Execution Vulnerability

10. CVE-2026-45463 Microsoft Office Remote Code Execution Vulnerability
11. CVE-2026-45461 Microsoft Office Remote Code Execution Vulnerability
12. CVE-2026-45458 Microsoft Outlook and Word Remote Code Execution Vulnerability
13. CVE-2026-45456 Microsoft Outlook and Word Remote Code Execution Vulnerability
14. CVE-2026-44824 Microsoft Office Remote Code Execution Vulnerability
15. CVE-2026-44819 Microsoft Office Remote Code Execution Vulnerability
16. CVE-2026-45469 Microsoft Excel Remote Code Execution Vulnerability
17. CVE-2026-44823 Microsoft Excel Remote Code Execution Vulnerability
18. CVE-2026-44820 Microsoft Excel Remote Code Execution Vulnerability
19. CVE-2026-44818 Microsoft Excel Remote Code Execution Vulnerability
20. CVE-2026-44817 Microsoft Excel Remote Code Execution Vulnerability
21. CVE-2026-47298 Microsoft SharePoint Server Remote Code Execution Vulnerability
22. CVE-2026-45454 Microsoft SharePoint Remote Code Execution Vulnerability
23. CVE-2026-45643 Microsoft Word Remote Code Execution Vulnerability
24. CVE-2026-45486 Microsoft Word Remote Code Execution Vulnerability
25. CVE-2026-45471 Microsoft Word Remote Code Execution Vulnerability
26. CVE-2026-45457 Microsoft Word Remote Code Execution Vulnerability
27. CVE-2026-26142 Nuance PowerScribe Remote Code Execution Vulnerability
28. CVE-2026-48563 Remote Desktop Client Remote Code Execution Vulnerability
29. CVE-2026-47654 Remote Desktop Client Remote Code Execution Vulnerability
30. CVE-2026-47653 Remote Desktop Client Remote Code Execution Vulnerability

31. CVE-2026-47289 Remote Desktop Client Remote Code Execution Vulnerability
32. CVE-2026-44801 Remote Desktop Client Remote Code Execution Vulnerability
33. CVE-2026-44799 Remote Desktop Client Remote Code Execution Vulnerability
34. CVE-2026-42993 Remote Desktop Client Remote Code Execution Vulnerability
35. CVE-2026-42992 Remote Desktop Client Remote Code Execution Vulnerability
36. CVE-2026-42985 Remote Desktop Client Remote Code Execution Vulnerability
37. CVE-2026-42913 Remote Desktop Client Remote Code Execution Vulnerability
38. CVE-2026-42909 Remote Desktop Client Remote Code Execution Vulnerability
39. CVE-2026-45641 Windows Hyper-V Remote Code Execution Vulnerability
40. CVE-2026-45635 Windows UPnP Device Host Remote Code Execution Vulnerability
41. CVE-2026-45599 Windows UPnP Device Host Remote Code Execution Vulnerability
42. CVE-2026-42987 Windows Deployment Services (WDS) Remote Code Execution
43. CVE-2026-44815 DHCP Client Service Remote Code Execution Vulnerability
44. CVE-2026-47291 HTTP.sys Remote Code Execution Vulnerability
45. CVE-2026-47652 Windows Hyper-V Remote Code Execution Vulnerability
46. CVE-2026-45607 Windows Hyper-V Remote Code Execution Vulnerability
47. CVE-2026-47288 Windows Kerberos Key Distribution Center (KDC) Remote Code Execution

48. CVE-2026-45657 Windows Kernel Remote Code Execution Vulnerability
49. CVE-2026-48574 Windows Media Remote Code Execution Vulnerability
50. CVE-2026-45636 Windows NTFS Remote Code Execution Vulnerability
51. CVE-2026-42981 Windows Performance Monitor Remote Code Execution Vulnerability
52. CVE-2026-42974 Windows Performance Monitor Remote Code Execution Vulnerability
53. CVE-2024-43582 Remote Desktop Protocol Server Remote Code Execution Vulnerability
54. CVE-2024-49123 Windows Remote Desktop Services Remote Code Execution Vulnerability
55. CVE-2026-44812 Windows Graphics Component Remote Code Execution Vulnerability
56. CVE-2026-44803 Windows Graphics Component Remote Code Execution Vulnerability

23. 67 פגיעויות ברכיבים/תוכנות הבאות עלולות לאפשר העלאת הרשאות:

1. CVE-2026-45490 .NET SDK Elevation of Privilege Vulnerability
2. CVE-2026-42836 Windows Function Discovery Service (fdwsd.dll) Elevation of Privilege Vulnerability
3. CVE-2026-45476 Microsoft Azure Network Adapter Elevation of Privilege Vulnerability
4. CVE-2026-33828 Windows Device Health Attestation (DHA) Elevation of Privilege Vulnerability
5. CVE-2026-45647 Microsoft Defender for Endpoint for Mac Elevation of Privilege Vulnerability
6. CVE-2026-40371 Microsoft Dynamics 365 (on-premises) Elevation of Privilege Vulnerability
7. CVE-2026-45504 Microsoft Exchange Server Elevation of Privilege Vulnerability

8. CVE-2026-42986 Microsoft Graphics Component Elevation of Privilege Vulnerability
9. CVE-2026-41092 Microsoft Kinect Elevation of Privilege Vulnerability
10. CVE-2026-45644 Microsoft Live Share Canvas SDK Elevation of Privilege Vulnerability
11. CVE-2026-47293 Microsoft Office Click-To-Run Elevation of Privilege Vulnerability
12. CVE-2026-45484 Microsoft SharePoint Elevation of Privilege Vulnerability
13. CVE-2026-50512 Microsoft PC Manager Elevation of Privilege Vulnerability
14. CVE-2026-50511 Microsoft PC Manager Elevation of Privilege Vulnerability
15. CVE-2026-42902 Microsoft PowerToys Elevation of Privilege Vulnerability
16. CVE-2020-17103 Windows Cloud Files Mini Filter Driver Elevation of Privilege Vulnerability
17. CVE-2026-41108 Windows DNS Client Elevation of Privilege Vulnerability
18. CVE-2026-45597 Windows UI Automation Manager (uiamanager.dll) Elevation of Privilege Vulnerability
19. CVE-2026-47292 Visual Studio Code MSSQL Extension Remote Code Execution Vulnerability
20. CVE-2026-47281 Visual Studio Code Elevation of Privilege Vulnerability
21. CVE-2026-40376 Visual Studio Code Elevation of Privilege Vulnerability
22. CVE-2026-45638 Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability
23. CVE-2026-45603 Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability
24. CVE-2026-45601 Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability
25. CVE-2026-45598 Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability

26. CVE-2026-45596 Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability
27. CVE-2026-42911 Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability
28. CVE-2026-34335 Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability
29. CVE-2026-45640 Windows Bluetooth Port Driver Elevation of Privilege Vulnerability
30. CVE-2026-45605 Windows Bluetooth Service Elevation of Privilege Vulnerability
31. CVE-2026-45586 Windows Collaborative Translation Framework (CTFMON) Elevation of Privilege Vulnerability
32. CVE-2026-44809 Windows Common Log File System Driver Elevation of Privilege Vulnerability
33. CVE-2026-44810 Microsoft Cryptographic Services Elevation of Privilege Vulnerability
34. CVE-2026-45637 Microsoft DWM Core Library Elevation of Privilege Vulnerability
35. CVE-2026-44813 Windows DWM Core Library Elevation of Privilege Vulnerability
36. CVE-2026-44811 Windows DWM Core Library Elevation of Privilege Vulnerability
37. CVE-2026-44808 Windows DWM Core Library Elevation of Privilege Vulnerability
38. CVE-2026-44807 Windows DWM Core Library Elevation of Privilege Vulnerability
39. CVE-2026-44804 Windows DWM Core Library Elevation of Privilege Vulnerability

40. CVE-2026-44802 Windows DWM Core Library Elevation of Privilege Vulnerability
41. CVE-2026-42983 Windows DWM Core Library Elevation of Privilege Vulnerability
42. CVE-2026-42905 Windows DWM Core Library Elevation of Privilege Vulnerability
43. CVE-2026-42910 Windows Hotpatch Monitoring Service Elevation of Privilege Vulnerability
44. CVE-2026-45592 Windows Internet (wininet.dll) Elevation of Privilege Vulnerability
45. CVE-2026-48583 Windows Kernel Elevation of Privilege Vulnerability
46. CVE-2026-45653 Windows Kernel Elevation of Privilege Vulnerability
47. CVE-2026-42984 Windows Kernel Elevation of Privilege Vulnerability
48. CVE-2026-45600 Windows Kernel-Mode Driver Elevation of Privilege Vulnerability
49. CVE-2026-48565 Windows Narrator Braille Elevation of Privilege Vulnerability
50. CVE-2026-42980 NT OS Kernel Elevation of Privilege Vulnerability
51. CVE-2026-42916 NT OS Kernel Elevation of Privilege Vulnerability
52. CVE-2026-45487 Windows Program Compatibility Assistant Service Elevation of Privilege Vulnerability
53. CVE-2026-42837 Windows Projected File System Elevation of Privilege Vulnerability
54. CVE-2026-42828 Windows Projected File System Elevation of Privilege Vulnerability
55. CVE-2026-42991 Windows Push Notifications Elevation of Privilege Vulnerability
56. CVE-2026-42979 Windows Push Notifications Elevation of Privilege Vulnerability

57. CVE-2026-42978 Windows Push Notifications Elevation of Privilege Vulnerability
58. CVE-2026-42977 Windows Push Notifications Elevation of Privilege Vulnerability
59. CVE-2026-21530 Windows Rich Text Edit Elevation of Privilege Vulnerability
60. CVE-2026-45593 Windows SDK Elevation of Privilege Vulnerability
61. CVE-2026-48578 Secure Boot Security Feature Bypass Vulnerability
62. CVE-2026-47648 Windows Storage Elevation of Privilege Vulnerability
63. CVE-2026-42904 Windows TCP/IP Elevation of Privilege Vulnerability
64. CVE-2026-42912 Windows Telephony Service Elevation of Privilege Vulnerability
65. CVE-2026-40409 Windows Universal Disk Format File System Driver (UDFS) Elevation of Privilege Vulnerability
66. CVE-2026-40404 Windows Universal Disk Format File System Driver (UDFS) Elevation of Privilege Vulnerability
67. CVE-2026-42989 Winlogon Elevation of Privilege Vulnerability

24. **10 פגיעויות ברכיבים/תוכנות הבאות עלולות לאפשר מתקפת מניעת שירות:**

1. CVE-2026-45591 ASP.NET Core Denial of Service Vulnerability
2. CVE-2026-49160 HTTP.sys Denial of Service Vulnerability
3. CVE-2026-45606 Microsoft UxTheme Library (uxtheme.dll) Denial of Service Vulnerability
4. CVE-2026-20846 GDI+ Denial of Service Vulnerability
5. CVE-2026-42914 Windows Kerberos Denial of Service Vulnerability
6. CVE-2026-42903 Windows Kerberos Denial of Service Vulnerability
7. CVE-2026-44805 Windows Network Controller (NC) Host Agent Denial of Service Vulnerability
8. CVE-2025-21330 Windows Remote Desktop Services Denial of Service Vulnerability

9. CVE-2024-49075 Windows Remote Desktop Services Denial of Service Vulnerability
10. CVE-2026-42915 Windows TCP/IP Denial of Service Vulnerability

25. **10 פגיעויות ברכיבים/תוכנות הבאות עלולות לאפשר מעקף של מנגנון אבטחה:**

1. CVE-2026-45591 ASP.NET Core Denial of Service Vulnerability
2. CVE-2026-49160 HTTP.sys Denial of Service Vulnerability
3. CVE-2026-45606 Microsoft UxTheme Library (uxtheme.dll) Denial of Service Vulnerability
4. CVE-2026-20846 GDI+ Denial of Service Vulnerability
5. CVE-2026-42914 Windows Kerberos Denial of Service Vulnerability
6. CVE-2026-42903 Windows Kerberos Denial of Service Vulnerability
7. CVE-2026-44805 Windows Network Controller (NC) Host Agent Denial of Service Vulnerability
8. CVE-2025-21330 Windows Remote Desktop Services Denial of Service Vulnerability
9. CVE-2024-49075 Windows Remote Desktop Services Denial of Service Vulnerability
10. CVE-2026-42915 Windows TCP/IP Denial of Service 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.