BEACON LAB
C S I R T

CYBOLT
Security Innovation

Boletín de Alerta

Boletín Nro.: 2024-21
Fecha de publicación: 14/08/2024
Tema: Múltiples vulnerabilidades críticas en Windows
Traffic Light Protocol (TLP): White

Producto(s) afectado:

- Multiples productos de Microsoft

Descripción

Este mes, Microsoft ha lanzado un parche que corrige 90 nuevas vulnerabilidades que afectan a diversos productos, incluyendo Windows y sus componentes, Office y Office Components, .NET y Visual Studio, Azure, Co-Pilot, Microsoft Dynamics, Teams y Secure Boot.

De las actualizaciones publicadas, siete están clasificadas como críticas, 79 como importantes y una como moderada en gravedad, algunas de ellas con explotación activa.

Puedes consultar la lista completa de CVE publicada por Microsoft en el siguiente enlace: https://msrc.microsoft.com/update-guide/releaseNote/2024-Aug.

CVE	Title	Severity	CVSS	Public	Exploited	Type
CVE-2024-38189	Microsoft Project Remote Code Execution Vulnerability	Important	8.8	No	Yes	RCE
CVE-2024-38178	Scripting Engine Memory Corruption Vulnerability	Important	7.5	No	Yes	RCE
CVE-2024-38193	Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability	Important	7.8	No	Yes	EoP
CVE-2024-38106	Windows Kernel Elevation of Privilege Vulnerability	Important	7	No	Yes	EoP
CVE-2024-38107	Windows Power Dependency Coordinator Elevation of Privilege Vulnerability	Important	7.8	No	Yes	EoP
CVE-2024-38213	Windows Mark of the Web Security Feature Bypass Vulnerability	Moderate	6.5	No	Yes	SFB
CVE-2024-38200	Microsoft Office Spoofing Vulnerability	Important	7.5	Yes	No	Spoofing
CVE-2024-38199	Windows Line Printer Daemon (LPD) Service Remote Code Execution Vulnerability	Important	9.8	Yes	No	RCE
CVE-2024-21302	Windows Secure Kernel Mode Elevation of Privilege Vulnerability	Important	6.7	Yes	No	EoP
CVE-2024-38202	Windows Update Stack Elevation of Privilege Vulnerability	Important	7.3	Yes	No	EoP

Imagen 1 Tabla de vulnerabilidades de seguridad en la actualización de agosto de 2024 (Zero Day Initiative, 2024).

A continuación, se destacan algunas de las vulnerabilidades más relevantes:

- CVE-2024-38063: Ejecución remota de código en Windows TCP/IP.
  Es una vulnerabilidad crítica de RCE con una puntuación CVSSv3 de 9.8, clasificada como "Explotación más probable". Un atacante podría explotarla de forma remota enviando paquetes IPv6 especialmente diseñados a un host.

- CVE-2024-38140: Ejecución remota de código en Windows Reliable Multicast Transport Driver (RMCAST).
  Otra vulnerabilidad crítica de RCE, con una puntuación CVSSv3 de 9.8. Un atacante no autenticado podría explotarla enviando paquetes diseñados a un socket de multidifusión general pragmática de Windows (PGM), sin necesidad de interacción del usuario.

- CVE-2024-38199: Ejecución remota de código en el servicio LPD (Line Printer Daemon) de Windows.
  Esta vulnerabilidad tiene una puntuación CVSSv3 de 9.8 y está clasificada como "Explotación poco probable". Un atacante remoto podría explotarla enviando una

tarea de impresión maliciosa al servicio LPD, lo que podría resultar en la ejecución remota de comandos en el servidor.

- CVE-2024-38108: Vulnerabilidad de suplantación de identidad en Azure Stack Hub. Esta vulnerabilidad de suplantación de identidad tiene una puntuación CVSSv3 de 9.3. Un atacante no autenticado podría explotarla para ejecutar código malicioso en el navegador de una víctima, aprovechando una identidad implícita de la máquina virtual.

- CVE-2024-38109: Vulnerabilidad de elevación de privilegios en bots de Azure Health. Clasificada como crítica, con una puntuación CVSSv3 de 9.1, esta vulnerabilidad SSRF podría permitir a un atacante aumentar los privilegios en Azure Health Bot.

Este resumen destaca la importancia de aplicar las actualizaciones correspondientes para mitigar los riesgos asociados a estas vulnerabilidades.

Solución

Asegúrate de instalar la actualización de seguridad correspondiente. Microsoft detalla los diversos métodos para realizar estas actualizaciones en el siguiente enlace: https://msrc.microsoft.com/update-guide/releaseNote/2024-Aug

Información adicional:

- https://msrc.microsoft.com/update-guide/releaseNote/2024-Aug
- https://www.incibe.es/incibe-cert/alerta-temprana/avisos/actualizaciones-de-seguridad-de-microsoft-de-agosto-de-2024
- https://www.tenable.com/blog/microsofts-august-2024-patch-tuesday-addresses-88-cves
- https://www.tenable.com/blog/microsofts-august-2024-patch-tuesday-addresses-88-cves
- https://www.bleepingcomputer.com/news/microsoft/microsoft-august-2024-patch-tuesday-fixes-9-zero-days-6-exploited/
- https://www.zerodayinitiative.com/blog/2024/8/13/the-august-2024-security-update-review

BEACON LAB
C S I R T

CYBOLT
Security Innovation

info@beaconlab.mx

beaconlab.mx

contact@cybolt.com

cybolt.com