BEACON LAB
C S I R T

CYBOLT
Security Innovation

Boletín de Alerta

Boletín Nro.: 2024-30
Fecha de publicación: 10/09/2024
Tema: Múltiples vulnerabilidades críticas en Windows
Traffic Light Protocol (TLP): White

Producto(s) afectado:

- Múltiples productos de Microsoft

Descripción

Este mes, Microsoft solucionó un total de 79 vulnerabilidades. incluidas 4 Zero-Days: CVE-2024-43491, CVE-2024-38014, CVE-2024-38226 y CVE-2024-38217, las mismas estaban siendo explotadas activamente. Las mismas afectan a varios productos como Microsoft SharePoint Server, Azure Stack y Windows Installer.

De las vulnerabilidades publicadas por Microsoft en su parche Mensual de los Martes (Microsoft September 2024 Patch Tuesday fixes), 7 fueron clasificadas como críticas, varias de ellas son de ejecución remota de código (RCE).

CVE	Title	Severity	CVSS	Public	Exploited	XI	Type
CVE-2024-38217	Windows Mark of the Web Security Feature Bypass Vulnerability	Important	5.4	Yes	Yes	0	SFB
CVE-2024-43491 †	Microsoft Windows Update Remote Code Execution Vulnerability	Critical	9.8	No	Yes	0	RCE
CVE-2024-38226	Microsoft Publisher Security Features Bypass Vulnerability	Important	7.3	No	Yes	0	SFB
CVE-2024-38014	Windows Installer Elevation of Privilege Vulnerability	Important	7.8	No	Yes	0	EoP
CVE-2024-43461	Windows MSHTML Platform Spoofing Vulnerability	Important	8.8	No	Disputed	1	Spoofing
CVE-2024-38216	Azure Stack Hub Elevation of Privilege Vulnerability	Critical	8.2	No	No	2	EoP
CVE-2024-38220	Azure Stack Hub Elevation of Privilege Vulnerability	Critical	9	No	No	2	EoP
CVE-2024-38194	Azure Web Apps Elevation of Privilege Vulnerability	Critical	8.4	No	No	2	EoP
CVE-2024-38018	Microsoft SharePoint Server Remote Code Execution Vulnerability	Critical	8.8	No	No	1	RCE
CVE-2024-43464	Microsoft SharePoint Server Remote Code Execution Vulnerability	Critical	7.2	No	No	1	RCE
CVE-2024-38119	Windows Network Address Translation (NAT) Remote Code Execution Vulnerability	Critical	7.5	No	No	2	RCE

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

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

- CVE-2024-43491 – Windows Update Remote Code Execution (RCE): Esta vulnerabilidad crítica (CVSS 9.8) afecta a la funcionalidad de Windows Update en versiones antiguas de Windows 10 (v1507). Permite a los atacantes ejecutar código remoto aprovechando un fallo en la actualización del stack de servicio. Es particularmente peligrosa porque está siendo explotada activamente.

- CVE-2024-38217 – Mark of the Web (MOTW) Security Feature Bypass: Esta vulnerabilidad, que también está siendo explotada, permite a los atacantes eludir las defensas de MOTW, que se encargan de identificar archivos descargados de Internet. Con una puntuación de 5.4 CVSS, aunque no es crítica, su explotación activa la hace relevante para entornos donde se manejan muchos archivos externos.

- CVE-2024-38018 – Microsoft SharePoint Server RCE: Esta vulnerabilidad afecta a SharePoint Server y permite la ejecución remota de código con permisos mínimos de miembro del sitio. Con un CVSS de 8.8, es crítica porque facilita la inyección y ejecución de código arbitrario si se manipulan archivos maliciosos en la plataforma.

- CVE-2024-38014 – Windows Installer Elevation of Privilege: Esta vulnerabilidad (CVSS 7.3) permite a un atacante elevar privilegios en sistemas Windows a nivel de SYSTEM, siendo crítica para entornos donde se requiere proteger la integridad de los sistemas operativos Windows.

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

Recomendamos aplicar las actualizaciones correspondientes para mitigar los riesgos asociados a estas vulnerabilidades los más pronto posible, especialmente aquellas que están siendo explotadas activamente.

Solución

Asegúrate de instalar la actualización de seguridad correspondiente. Microsoft detalla los diversos métodos para realizar estas actualizaciones en los siguientes enlaces:

- https://msrc.microsoft.com/update-guide/releaseNote/2024-Sep
- https://support.microsoft.com/en-us/topic/september-10-2024-kb5043076-os-builds-22621-4169-and-22631-4169-215aad1e-3f3f-44bd-9868-91a2bd450a07
- https://support.microsoft.com/en-us/topic/september-10-2024-kb5043080-os-build-26100-1742-407666c8-6b6d-4561-a982-abce4e7c2efb
- https://support.microsoft.com/en-us/topic/september-10-2024-kb5043064-os-builds-19044-4894-and-19045-4894-cd14b547-a3f0-4b8f-b037-4ae3ce83a781

Información adicional:

- https://msrc.microsoft.com/update-guide/releaseNote/2024-Sep
- Microsoft September 2024 Patch Tuesday fixes 4 zero-days, 79 flaws (bleepingcomputer.com)
- https://www.zerodayinitiative.com/blog/2024/9/10/the-september-2024-security-update-review
- https://blog.qualys.com/vulnerabilities-threat-research/2024/09/10/microsoft-and-adobe-patch-tuesday-september-2024-security-update-review#:~:text=and%20their%20implications.-,Microsoft%20Patch%20Tuesday%20for%20September%202024,be%20exploited%20in%20the%20wild.
- https://www.tenable.com/blog/microsofts-september-2024-patch-tuesday-addresses-79-cves-cve-2024-43491

BEACON LAB
C S I R T

CYBOLT
Security Innovation

info@beaconlab.mx

beaconlab.mx

contact@cybolt.com

cybolt.com