Actualización de seguridad de Microsoft-Abril 2024

CYBERZAINTZA-ACTUALIZACIONES-MICROSOFT-2024-ABRIL

TLP: CLEAR

www.ciberseguridad.eus

TABLA DE CONTENIDO

Cláusula de exención de responsabilidad

El presente documento se proporciona con el objeto de divulgar las alertas que la Agencia de Ciberseguridad Vasca considera necesarias en favor de la seguridad de las organizaciones y de la ciudadanía interesada. En ningún caso la Agencia de Ciberseguridad Vasca puede ser considerado responsable de posibles daños que, de forma directa o indirecta, de manera fortuita o extraordinaria pueda ocasionar el uso de la información revelada, así como de las tecnologías a las que se haga referencia tanto de la web de la Agencia de Ciberseguridad Vasca como de información externa a la que se acceda mediante enlaces a páginas webs externas, a redes sociales, a productos de software o a cualquier otra información que pueda aparecer en la alerta o en la web de la Agencia de Ciberseguridad Vasca. En todo caso, los contenidos de la alerta y las contestaciones que pudieran darse a través de los diferentes correos electrónicos son opiniones y recomendaciones acorde a los términos aquí recogidos no pudiendo derivarse efecto jurídico vinculante derivado de la información comunicada.

Cláusula de prohibición de venta

Queda terminantemente prohibida la venta u obtención de cualquier beneficio económico, sin perjuicio de la posibilidad de copia, distribución, difusión o divulgación del presente documento.

1. Resumen ejecutivo

Microsoft ha publicado las actualizaciones de seguridad del mes de **abril de 2024** en las que se corrigen **157 vulnerabilidades**, siendo **3** de ellas calificadas como **críticas**, **145** como **importantes, 3 moderadas, 1 baja** y **5 sin un valor asignado** que afectan al navegador Edge basado en Chromium.

Estas vulnerabilidades afectan a productos como Microsoft Defender for IoT, Microsoft Office Excel, Azure Private 5G Core, Windows BitLocker, Windows Secure Boot, Microsoft Office Outlook, Windows Kerberos y Azure Migrate, entre otros.

Por otra parte, las **vulnerabilidades identificadas con una posibilidad potencial de explotación** son CVE-2024-29988, CVE-2024-26256, CVE-2024-26158, CVE-2024-26218, CVE-2024-26241, CVE-2024-26211, CVE-2024-26230, CVE-2024-26239, CVE-2024-26212, CVE-2024-28921, CVE-2024-28903, CVE-2024-26234, CVE-2024-26209, CVE-2024-29056.

La clasificación de las vulnerabilidades según su descripción es la siguiente:

- 67 vulnerabilidades de ejecución remota de código.
- 31 vulnerabilidades de elevación de privilegios.
- 27 vulnerabilidades de bypass.
- 12 vulnerabilidades de divulgación de información.
- 7 vulnerabilidades de denegación de servicio.
- 5 vulnerabilidades de spoofing (suplantación).
- 2 vulnerabilidades en CBL-Mariner.
- 1 vulnerabilidad use after free.
- 1 vulnerabilidad de acceso a memoria fuera de límites
- 1 vulnerabilidad de implementación inapropiada.
- 1 vulnerabilidad inyección de historial de sucursales.
- 1 vulnerabilidad de desbordamiento de búfer de pila.
- 1 vulnerabilidad de anulación del administrador de arranque.

2. Recursos afectados

Las actualizaciones de seguridad del mes de abril de 2024 están asociadas a vulnerabilidades que afectan a los siguientes productos:

- Windows BitLocker
- Windows Secure Boot
- Microsoft Office Outlook
- Windows Remote Procedure Call
- Azure Private 5G Core
- Windows Kernel
- Microsoft Defender for IoT
- .NET and Visual Studio
- Azure Compute Gallery
- Windows Authentication Methods
- Microsoft Install Service
- Windows DWM Core Library
- Windows Routing and Remote Access Service (RRAS)
- Windows Kerberos
- Azure Migrate
- Windows DHCP Server
- Windows Remote Access Connection Manager
- Windows Message Queuing
- Windows Local Security Authority Subsystem Service (LSASS)
- Microsoft WDAC OLE DB provider for SQL
- Windows Remote Access Connection Manager
- Microsoft Brokering File System
- Microsoft WDAC ODBC Driver
- Windows File Server Resource Management Service
- Windows Remote Access Connection Manager
- Windows HTTP.sys
- Windows Mobile Hotspot
- Role: DNS Server

- Windows Distributed File System (DFS)r
- Windows Cryptographic Services
- Windows Remote Access Connection Manager
- Windows Proxy Driver
- Windows Update Stack
- Windows Defender Credential Guard
- Windows Remote Access Connection Manager
- Windows Win32K - ICOMP
- Windows Telephony Server
- Windows USB Print Driver
- Microsoft WDAC OLE DB provider for SQL
- Windows Kernel
- Windows Kerberos
- Microsoft Office SharePoint
- Windows Internet Connection Sharing (ICS)
- Windows Virtual Machine Bus
- Windows Remote Access Connection Manager
- Windows Compressed Folder
- Microsoft Office Excel
- Windows Remote Access Connection Manager
- Windows Secure Boot
- Microsoft Brokering File System
- SQL Server
- Azure Arc
- Windows Secure Boot
- Microsoft Edge (Chromium-based)
- Windows Cryptographic Services
- Windows Storage
- Windows Authentication Methods
- Azure AI Search
- Role: Windows Hyper-V

- Windows Distributed File System (DFS)
- Internet Shortcut Files
- Azure Monitor
- Microsoft Azure Kubernetes Service
- Azure SDK
- Azure

3. Análisis técnico

A continuación, los detalles de las vulnerabilidades de más relevancia corregidas en esta actualización, que son los siguientes:

CVE-2024-21323: vulnerabilidad de ejecución remota de código en Microsoft Defender para IoT. La explotación exitosa de esta vulnerabilidad requiere que el atacante pueda enviar un paquete de actualización malicioso al sensor de Defender for IoT a través de la red. Para lograr esto, el atacante primero tendría que autenticarse y obtener los permisos necesarios para iniciar el proceso de actualización. Para aprovechar con éxito esta vulnerabilidad de travesía de directorios se requiere que un atacante envíe un archivo tar al sensor de Defender for IoT. Una vez completado el proceso de extracción, el atacante podría enviar paquetes de actualización no firmados y sobrescribir cualquier archivo que elijan.

TTP

- Táctica TA0003 – Persistence
  - Técnica T1505 – Server Software Component
  - Cumplimiento – ENS
    - SI-7, SI-4, SI-14, SC-16, SA-11, SA-10, RA-5, IA-2, CM-8, CM-6, CM-5, CM-2, CM-11, CA-8, AC-6, AC-5, AC-3, AC-2, AC-16, SR-6, SR-4, SR-11.
- Táctica TA0004 – Privilege Escalation
  - Técnica T1068 – Exploitation for Privilege Escalation
  - Cumplimiento – ENS
    - SI-3, SI-2, SC-7, SC-39, SC-35, SC-30, SC-3, SC-29, SC-26, SC-2, SC-18, RA-5, RA-10, CM-8, CM-7, CM-6, CM-2, CA-8, CA-7, AC-6, AC-4, AC-2, SI-7, SI-5, SI-4.
- Táctica TA0008 – Lateral Movement
  - Técnica T1210 – Exploitation of Remote Services
  - Cumplimiento – ENS
    - SC-46, SC-39, SC-35, SC-30, SC-3, SC-29, SC-26, SC-2, SC-18, RA-5, RA-10, IA-8, IA-2, CM-8, CM-7, CM-6, CM-5, CM-2, CA-8, CA-7, CA-2, AC-6, AC-5, AC-4, AC-3, AC-2, SI-7, SI-5, SI-4, SI-3, SI-2, SC-7.
- Táctica TA0011 – Command and Control
  - Técnica T1105 – Ingress Tool Transfer
  - Cumplimiento – ENS
    - CM-7, CM-6, CM-2, CA-7, AC-4, SI-4, SI-3, SC-7.

La métrica de evaluación de la vulnerabilidad se compone de:

CWE 36: Absolute Path Traversal

CVSS Base: **8.8**

CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

- **Vector de ataque**: **Red**
- **Complejidad del ataque**: **Baja**
- **Privilegios requeridos: Bajos**
- **Interacción con el usuario**: **Ninguna**
- **Alcance**: Sin cambios
- **Confidencialidad: Alta**
- **Integridad: Alta**
- **Disponibilidad: Alta**

CVE-2024-29053: vulnerabilidad de ejecución remota de código de Microsoft Defender para IoT. Cualquier atacante autenticado podría desencadenar esta vulnerabilidad. No requiere privilegios de administrador ni otros privilegios elevados. Un atacante autenticado con acceso a la función de carga de archivos podría aprovechar esta vulnerabilidad de recorrido de ruta cargando archivos maliciosos en ubicaciones confidenciales del servidor.

TTP

- Táctica TA0003 – Persistence
  - Técnica T1505 – Server Software Component
  - Cumplimiento – ENS
    - SI-7, SI-4, SI-14, SC-16, SA-11, SA-10, RA-5, IA-2, CM-8, CM-6, CM-5, CM-2, CM-11, CA-8, AC-6, AC-5, AC-3, AC-2, AC-16, SR-6, SR-4, SR-11.
- Táctica TA0004 – Privilege Escalation
  - Técnica T1068 – Exploitation for Privilege Escalation
  - Cumplimiento – ENS
    - SI-3, SI-2, SC-7, SC-39, SC-35, SC-30, SC-3, SC-29, SC-26, SC-2, SC-18, RA-5, RA-10, CM-8, CM-7, CM-6, CM-2, CA-8, CA-7, AC-6, AC-4, AC-2, SI-7, SI-5, SI-4.
- Táctica TA0008 – Lateral Movement
  - Técnica T1210 – Exploitation of Remote Services
  - Cumplimiento – ENS
    - SC-46, SC-39, SC-35, SC-30, SC-3, SC-29, SC-26, SC-2, SC-18, RA-5, RA-10, IA-8, IA-2, CM-8, CM-7, CM-6, CM-5, CM-2, CA-8, CA-7, CA-2, AC-6, AC-5, AC-4, AC-3, AC-2, SI-7, SI-5, SI-4, SI-3, SI-2, SC-7.
- Táctica TA0011 – Command and Control
  - Técnica T1105 – Ingress Tool Transfer
  - Cumplimiento – ENS
    - CM-7, CM-6, CM-2, CA-7, AC-4, SI-4, SI-3, SC-7.

La métrica de evaluación de la vulnerabilidad se compone de:

CWE 36: Absolute Path Traversal

CVSS Base: **8.8**

CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

- **Vector de ataque**: **Red**
- **Complejidad del ataque**: **Baja**
- **Privilegios requeridos: Bajos**
- **Interacción con el usuario**: **Ninguna**
- **Alcance**: Sin cambios
- **Confidencialidad: Alta**
- **Integridad: Alta**
- **Disponibilidad: Alta**

CVE-2024-21322: vulnerabilidad de ejecución remota de código de Microsoft Defender para IoT. La explotación exitosa de esta vulnerabilidad requiere que el atacante sea un administrador de la aplicación web. Como es la mejor práctica, se deben llevar a cabo validaciones y auditorías periódicas de los grupos administrativos.

TTP

- Táctica TA0001 – Initial Access
  - Técnica T1078 – Valid Accounts
  - Cumplimiento – ENS
    - SI-4, SC-28, SA-8, SA-4, SA-3, SA-17, SA-16, SA-15, SA-11, SA-10, RA-5, IA-5, IA-2, IA-12, CM-6, CM-5, CA-8, CA-7, AC-6, AC-5, AC-3, AC-2, SR-6.
- Táctica TA0004 – Privilege Escalation
  - Técnica T1068 – Exploitation for Privilege Escalation
  - Cumplimiento – ENS
    - SI-3, SI-2, SC-7, SC-39, SC-35, SC-30, SC-3, SC-29, SC-26, SC-2, SC-18, RA-5, RA-10, CM-8, CM-7, CM-6, CM-2, CA-8, CA-7, AC-6, AC-4, AC-2, SI-7, SI-5, SI-4.
- Táctica TA0008 – Defense Evasion
  - Técnica T1140 – Deobfuscate/Decode Files or Information

La métrica de evaluación de la vulnerabilidad se compone de:

CWE 77: Improper Neutralization of Special Elements used in a Command (Command Injection)

CVSS Base: **7.2**

CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H

- **Vector de ataque**: **Red**
- **Complejidad del ataque**: **Baja**

- **Privilegios requeridos:** Altos
- **Interacción con el usuario**: **Ninguna**
- **Alcance**: Sin cambios
- **Confidencialidad: Alta**
- **Integridad: Alta**
- **Disponibilidad: Alta**

A continuación, se detalla la lista con todas las vulnerabilidades identificadas:

➢ Las vulnerabilidades identificadas por los CVE marcados en color rojo representan a aquellas que se conoce que están siendo explotadas, o que tienen el potencial de serlo, en función del estado de la amenaza. Este riesgo de explotación se encuentra presente en la última versión del software suministrado por el fabricante.

CVE	Descripción	Severidad	Divulgado	Explotado	CVSS	Soluciones alternativas
CVE-2024-21323	Vulnerabilidad de ejecución remota de código de Microsoft Defender para IoT	**Crítica**	No	No	8.8	No
CVE-2024-29053	Vulnerabilidad de ejecución remota de código de Microsoft Defender para IoT	**Crítica**	No	No	8.8	No
CVE-2024-21322	Vulnerabilidad de ejecución remota de código de Microsoft Defender para IoT	**Crítica**	No	No	7.2	No
CVE-2024-29990	Vulnerabilidad de elevación confidencial de privilegios de contenedor de Microsoft Azure Kubernetes Service	Importante	No	No	9.0	No

CVE-2024-26179	Vulnerabilidad de ejecución remota de código del servicio de enrutamiento y acceso remoto (RRAS) de Windows	Importante	No	No	8.8	No
CVE-2024-26200	Vulnerabilidad de ejecución remota de código del servicio de enrutamiento y acceso remoto (RRAS) de Windows	Importante	No	No	8.8	No
CVE-2024-26205	Vulnerabilidad de ejecución remota de código del servicio de enrutamiento y acceso remoto (RRAS) de Windows	Importante	No	No	8.8	No
CVE-2024-28906	Vulnerabilidad del controlador OLE DB de Microsoft para la ejecución remota de código de SQL Server	Importante	No	No	8.8	No
CVE-2024-28908	Vulnerabilidad del controlador OLE DB de Microsoft para la ejecución remota de código de SQL Server	Importante	No	No	8.8	No
CVE-2024-28909	Vulnerabilidad del controlador OLE DB de	Importante	No	No	8.8	No

	Microsoft para la ejecución remota de código de SQL Server					
CVE-2024-28910	Vulnerabilidad del controlador OLE DB de Microsoft para la ejecución remota de código de SQL Server	Importante	No	No	8.8	No
CVE-2024-28911	Vulnerabilidad del controlador OLE DB de Microsoft para la ejecución remota de código de SQL Server	Importante	No	No	8.8	No
CVE-2024-28912	Vulnerabilidad del controlador OLE DB de Microsoft para la ejecución remota de código de SQL Server	Importante	No	No	8.8	No
CVE-2024-28913	Vulnerabilidad del controlador OLE DB de Microsoft para la ejecución remota de código de SQL Server	Importante	No	No	8.8	No
CVE-2024-28914	Vulnerabilidad del controlador OLE DB de Microsoft para la ejecución remota de código de SQL Server	Importante	No	No	8.8	No

CVE-2024-28915	Vulnerabilidad del controlador OLE DB de Microsoft para la ejecución remota de código de SQL Server	Importante	No	No	8.8	No
CVE-2024-28929	Vulnerabilidad del controlador ODBC de Microsoft para la ejecución remota de código de SQL Server	Importante	No	No	8.8	No
CVE-2024-28931	Vulnerabilidad del controlador ODBC de Microsoft para la ejecución remota de código de SQL Server	Importante	No	No	8.8	No
CVE-2024-28932	Vulnerabilidad del controlador ODBC de Microsoft para la ejecución remota de código de SQL Server	Importante	No	No	8.8	No
CVE-2024-28936	Vulnerabilidad del controlador ODBC de Microsoft para la ejecución remota de código de SQL Server	Importante	No	No	8.8	No
CVE-2024-28939	Vulnerabilidad del controlador OLE DB de Microsoft para la ejecución remota de	Importante	No	No	8.8	No

	código de SQL Server					
CVE-2024-28942	Vulnerabilidad del controlador OLE DB de Microsoft para la ejecución remota de código de SQL Server	Importante	No	No	8.8	No
CVE-2024-28945	Vulnerabilidad del controlador OLE DB de Microsoft para la ejecución remota de código de SQL Server	Importante	No	No	8.8	No
CVE-2024-29043	Vulnerabilidad del controlador ODBC de Microsoft para la ejecución remota de código de SQL Server	Importante	No	No	8.8	No
CVE-2024-29047	Vulnerabilidad del controlador OLE DB de Microsoft para la ejecución remota de código de SQL Server	Importante	No	No	8.8	No
CVE-2024-29988	Vulnerabilidad de omisión de la función de seguridad de aviso de SmartScreen	Importante	No	No	8.8	No
CVE-2024-20678	Vulnerabilidad de ejecución remota de código en tiempo de ejecución de	Importante	No	No	8.8	No

	llamadas a procedimientos remotos					
CVE-2024-26210	Vulnerabilidad de ejecución remota de código del proveedor OLE DB de Microsoft WDAC para SQL Server	Importante	No	No	8.8	No
CVE-2024-26244	Vulnerabilidad de ejecución remota de código del proveedor OLE DB de Microsoft WDAC para SQL Server	Importante	No	No	8.8	No
CVE-2024-26214	Microsoft WDAC SQL Server ODBC Driver Remote Code Execution Vulnerability	Importante	No	No	8.8	No
CVE-2024-28926	Vulnerabilidad del controlador OLE DB de Microsoft para la ejecución remota de código de SQL Server	Importante	No	No	8.8	No
CVE-2024-28927	Vulnerabilidad del controlador OLE DB de Microsoft para la ejecución remota de código de SQL Server	Importante	No	No	8.8	No
CVE-2024-28930	Vulnerabilidad del controlador ODBC de Microsoft para la ejecución	Importante	No	No	8.8	No

	remota de código de SQL Server					
CVE-2024-28933	Vulnerabilidad del controlador ODBC de Microsoft para la ejecución remota de código de SQL Server	Importante	No	No	8.8	No
CVE-2024-28934	Vulnerabilidad del controlador ODBC de Microsoft para la ejecución remota de código de SQL Server	Importante	No	No	8.8	No
CVE-2024-28935	Vulnerabilidad del controlador ODBC de Microsoft para la ejecución remota de código de SQL Server	Importante	No	No	8.8	No
CVE-2024-28937	Vulnerabilidad del controlador ODBC de Microsoft para la ejecución remota de código de SQL Server	Importante	No	No	8.8	No
CVE-2024-28938	Vulnerabilidad del controlador ODBC de Microsoft para la ejecución remota de código de SQL Server	Importante	No	No	8.8	No
CVE-2024-28940	Vulnerabilidad del controlador OLE DB de	Importante	No	No	8.8	No

	Microsoft para la ejecución remota de código de SQL Server					
CVE-2024-28941	Vulnerabilidad del controlador ODBC de Microsoft para la ejecución remota de código de SQL Server	Importante	No	No	8.8	No
CVE-2024-28943	Vulnerabilidad del controlador ODBC de Microsoft para la ejecución remota de código de SQL Server	Importante	No	No	8.8	No
CVE-2024-28944	Vulnerabilidad del controlador OLE DB de Microsoft para la ejecución remota de código de SQL Server	Importante	No	No	8.8	No
CVE-2024-29044	Vulnerabilidad del controlador OLE DB de Microsoft para la ejecución remota de código de SQL Server	Importante	No	No	8.8	No
CVE-2024-29046	Vulnerabilidad del controlador OLE DB de Microsoft para la ejecución remota de código de SQL Server	Importante	No	No	8.8	No

CVE-2024-29048	Vulnerabilidad del controlador OLE DB de Microsoft para la ejecución remota de código de SQL Server	Importante	No	No	8.8	No
CVE-2024-29982	Vulnerabilidad del controlador OLE DB de Microsoft para la ejecución remota de código de SQL Server	Importante	No	No	8.8	No
CVE-2024-29983	Vulnerabilidad del controlador OLE DB de Microsoft para la ejecución remota de código de SQL Server	Importante	No	No	8.8	No
CVE-2024-29984	Microsoft OLE DB Driver for SQL Server Remote Code Execution Vulnerability	Importante	No	No	8.8	No
CVE-2024-29985	Vulnerabilidad del controlador OLE DB de Microsoft para la ejecución remota de código de SQL Server	Importante	No	No	8.8	No
CVE-2024-29993	Vulnerabilidad de elevación de privilegios de Azure CycleCloud	Importante	No	No	8.8	No
CVE-2024-29050	Vulnerabilidad de ejecución remota de	Importante	No	No	8.4	No

	código de los Servicios criptográficos de Windows					
CVE-2024-29989	Vulnerabilidad de elevación de privilegios del agente de Azure Monitor	Importante	No	No	8.4	No
CVE-2024-20670	Vulnerabilidad de suplantación de identidad de Outlook para Windows	Importante	No	No	8.1	No
CVE-2024-26180	Vulnerabilidad de omisión de la función de seguridad de arranque seguro	Importante	No	No	8.0	No
CVE-2024-26189	Vulnerabilidad de omisión de la función de seguridad de arranque seguro	Importante	No	No	8.0	No
CVE-2024-26240	Vulnerabilidad de omisión de la función de seguridad de arranque seguro	Importante	No	No	8.0	No
CVE-2024-28925	Vulnerabilidad de omisión de la función de seguridad de arranque seguro	Importante	No	No	8.0	No
CVE-2024-26256	Vulnerabilidad de ejecución remota de código en libarchive	Importante	No	No	7.8	No
CVE-2024-26158	Vulnerabilidad de elevación de privilegios del servicio de instalación de Microsoft	Importante	No	No	7.8	No

CVE-2024-28920	Vulnerabilidad de omisión de la función de seguridad de arranque seguro	Importante	No	No	7.8	No
CVE-2024-28905	Vulnerabilidad de elevación de privilegios del sistema de archivos de intermediación de Microsoft	Importante	No	No	7.8	No
CVE-2024-20693	Vulnerabilidad de elevación de privilegios del kernel de Windows	Importante	No	No	7.8	No
CVE-2024-21447	Vulnerabilidad de elevación de privilegios de autenticación de Windows	Importante	No	No	7.8	No
CVE-2024-26175	Vulnerabilidad de omisión de la función de seguridad de arranque seguro	Importante	No	No	7.8	No
CVE-2024-26218	Vulnerabilidad de elevación de privilegios del kernel de Windows	Importante	No	No	7.8	No
CVE-2024-26241	Vulnerabilidad de elevación de privilegios de Win32k	Importante	No	No	7.8	No
CVE-2024-26229	Vulnerabilidad de elevación de privilegios del servicio CSC de Windows	Importante	No	No	7.8	No
CVE-2024-26235	Vulnerabilidad de elevación de privilegios de la pila de Windows Update	Importante	No	No	7.8	No

CVE-2024-26237	Vulnerabilidad de elevación de privilegios de Windows Defender Credential Guard	Importante	No	No	7.8	No
CVE-2024-26245	Vulnerabilidad de elevación de privilegios de Windows SMB	Importante	No	No	7.8	No
CVE-2024-26211	Vulnerabilidad de elevación de privilegios de Windows Remote Access Connection Manager	Importante	No	No	7.8	No
CVE-2024-26228	Vulnerabilidad de omisión de características de seguridad de los servicios criptográficos de Windows	Importante	No	No	7.8	No
CVE-2024-26230	Vulnerabilidad de elevación de privilegios del servidor de telefonía de Windows	Importante	No	No	7.8	No
CVE-2024-26239	Vulnerabilidad de elevación de privilegios del servidor de telefonía de Windows	Importante	No	No	7.8	No
CVE-2024-26257	Vulnerabilidad de ejecución remota de código de Microsoft Excel	Importante	No	No	7.8	No
CVE-2024-28904	Vulnerabilidad de elevación de privilegios del sistema de archivos de	Importante	No	No	7.8	No

	intermediación de Microsoft					
CVE-2024-28907	Vulnerabilidad de elevación de privilegios del sistema de archivos de intermediación de Microsoft	Importante	No	No	7.8	No
CVE-2024-29052	Vulnerabilidad de elevación de privilegios de almacenamiento de Windows	Importante	No	No	7.8	No
CVE-2024-29061	Vulnerabilidad de omisión de la función de seguridad de arranque seguro	Importante	No	No	7.8	No
CVE-2024-23593	**Lenovo**: vulnerabilidad que anula el Administrador de Arranque y pasar al Shell de UEFI	Importante	No	No	7.8	No
CVE-2024-26254	Vulnerabilidad de denegación de servicio de Microsoft Virtual Machine Bus (VMBus)	Importante	No	No	7.5	No
CVE-2024-28896	Vulnerabilidad de omisión de la función de seguridad de arranque seguro	Importante	No	No	7.5	No
CVE-2024-29045	Vulnerabilidad del controlador OLE DB de Microsoft para la ejecución remota de código de SQL Server	Importante	No	No	7.5	No

CVE-2024-26219	HTTP.sys Vulnerabilidad de denegación de servicio	Importante	No	No	7.5	No
CVE-2024-26248	Vulnerabilidad de elevación de privilegios de Windows Kerberos	Importante	No	No	7.5	No
CVE-2024-26212	Vulnerabilidad de denegación de servicio del servidor DHCP	Importante	No	No	7.5	No
CVE-2024-26215	Vulnerabilidad de denegación de servicio del servidor DHCP	Importante	No	No	7.5	No
CVE-2024-26194	Vulnerabilidad de omisión de la función de seguridad de arranque seguro	Importante	No	No	7.4	No
CVE-2024-21409	Vulnerabilidad de ejecución remota de código de .NET, .NET Framework y Visual Studio	Importante	No	No	7.3	No
CVE-2024-26232	Vulnerabilidad de ejecución remota de código de Microsoft Message Queue Server (MSMQ)	Importante	No	No	7.3	Sí
CVE-2024-29063	Vulnerabilidad de divulgación de información de búsqueda de Azure AI	Importante	No	No	7.3	No
CVE-2024-26216	Vulnerabilidad de elevación de privilegios del servicio de administración de recursos del	Importante	No	No	7.3	No

	servidor de archivos de Windows					
CVE-2024-29066	Vulnerabilidad de ejecución remota de código del sistema de archivos distribuido (DFS) de Windows	Importante	No	No	7.2	No
CVE-2024-21324	Vulnerabilidad de elevación de privilegios de Microsoft Defender para IoT	Importante	No	No	7.2	No
CVE-2024-26195	Vulnerabilidad de ejecución remota de código del servicio de servidor DHCP	Importante	No	No	7.2	No
CVE-2024-26202	Vulnerabilidad de ejecución remota de código del servicio de servidor DHCP	Importante	No	No	7.2	No
CVE-2024-26221	Vulnerabilidad de ejecución remota de código de Windows DNS Server	Importante	No	No	7.2	No
CVE-2024-26222	Vulnerabilidad de ejecución remota de código de Windows DNS Server	Importante	No	No	7.2	No
CVE-2024-26223	Vulnerabilidad de ejecución remota de código de	Importante	No	No	7.2	No

	Windows DNS Server					
CVE-2024-26224	Vulnerabilidad de ejecución remota de código de Windows DNS Server	Importante	No	No	7.2	No
CVE-2024-26227	Vulnerabilidad de ejecución remota de código de Windows DNS Server	Importante	No	No	7.2	No
CVE-2024-26231	Vulnerabilidad de ejecución remota de código de Windows DNS Server	Importante	No	No	7.2	No
CVE-2024-26233	Windows DNS Server Remote Code Execution Vulnerability	Importante	No	No	7.2	No
CVE-2024-26208	Vulnerabilidad de ejecución remota de código de Microsoft Message Queue Server (MSMQ)	Importante	No	No	7.2	No
CVE-2024-29055	Vulnerabilidad de elevación de privilegios de Microsoft Defender para IoT	Importante	No	No	7.2	No
CVE-2024-29054	Vulnerabilidad de elevación de privilegios de Microsoft Defender para IoT	Importante	No	No	7.2	No
CVE-2024-20688	Vulnerabilidad de omisión de la función de	Importante	No	No	7.1	No

	seguridad de arranque seguro					
CVE-2024-20689	Vulnerabilidad de omisión de la función de seguridad de arranque seguro	Importante	No	No	7.1	No
CVE-2024-29062	Vulnerabilidad de omisión de la función de seguridad de arranque seguro	Importante	No	No	7.1	No
CVE-2024-26243	Vulnerabilidad de elevación de privilegios del controlador de impresión USB de Windows	Importante	No	No	7.0	No
CVE-2024-26236	Vulnerabilidad de elevación de privilegios de la pila de Windows Update	Importante	No	No	7.0	No
CVE-2024-26242	Vulnerabilidad de elevación de privilegios del servidor de telefonía de Windows	Importante	No	No	7.0	No
CVE-2024-26213	Vulnerabilidad de elevación de privilegios del sistema de archivos de intermediación de Microsoft	Importante	No	No	7.0	No
CVE-2024-26252	Vulnerabilidad de ejecución remota de código de Windows rndismp6.sys	Importante	No	No	6.8	No
CVE-2024-26253	Vulnerabilidad de ejecución remota de código de	Importante	No	No	6.8	No

	Windows rndismp6.sys					
CVE-2024-26168	Vulnerabilidad de omisión de la función de seguridad de arranque seguro	Importante	No	No	6.8	No
CVE-2024-26251	Vulnerabilidad de suplantación de identidad de Microsoft SharePoint Server	Importante	No	No	6.8	No
CVE-2024-28897	Vulnerabilidad de omisión de la función de seguridad de arranque seguro	Importante	No	No	6.8	No
CVE-2024-20669	Vulnerabilidad de omisión de la función de seguridad de arranque seguro	Importante	No	No	6.7	No
CVE-2024-26250	Vulnerabilidad de omisión de la función de seguridad de arranque seguro	Importante	No	No	6.7	No
CVE-2024-28921	Vulnerabilidad de omisión de la función de seguridad de arranque seguro	Importante	No	No	6.7	No
CVE-2024-28919	Vulnerabilidad de omisión de la función de seguridad de arranque seguro	Importante	No	No	6.7	No
CVE-2024-28903	Vulnerabilidad de omisión de la función de seguridad de arranque seguro	Importante	No	No	6.7	No
CVE-2024-26171	Vulnerabilidad de omisión de la función de	Importante	No	No	6.7	No

	seguridad de arranque seguro					
CVE-2024-26234	Vulnerabilidad de suplantación de identidad del controlador proxy	Importante	No	No	6.7	No
CVE-2024-28924	Vulnerabilidad de omisión de la función de seguridad de arranque seguro	Importante	No	No	6.7	No
CVE-2024-21424	Vulnerabilidad de elevación de privilegios de Azure Compute Gallery	Importante	No	No	6.5	No
CVE-2024-26183	Vulnerabilidad de denegación de servicio de Windows Kerberos	Importante	No	No	6.5	No
CVE-2024-26226	Vulnerabilidad de divulgación de información del sistema de archivos distribuido (DFS) de Windows	Importante	No	No	6.5	No
CVE-2024-28923	Vulnerabilidad de omisión de la función de seguridad de arranque seguro	Importante	No	No	6.4	No
CVE-2024-23594	**Lenovo**: Desbordamiento de búfer de pila en LenovoBT.efi	Importante	No	No	6.4	No
CVE-2024-26193	Vulnerabilidad de ejecución remota de código de Azure Migrate	Importante	No	No	6.4	No

CVE-2024-28898	Vulnerabilidad de omisión de la función de seguridad de arranque seguro	Importante	No	No	6.3	No
CVE-2024-29064	Vulnerabilidad de denegación de servicio de Windows Hyper-V	Importante	No	No	6.2	No
CVE-2024-28917	Vulnerabilidad de elevación de privilegios de ámbito de clúster de extensión de Kubernetes habilitada para Azure Arc	Importante	No	No	6.2	No
CVE-2024-20665	Vulnerabilidad de omisión de características de seguridad de BitLocker	Importante	No	No	6.1	No
CVE-2024-26255	Vulnerabilidad de divulgación de información de Windows Remote Access Connection Manager	Importante	No	No	5.5	No
CVE-2024-26172	Vulnerabilidad de divulgación de información de la biblioteca principal de Windows DWM	Importante	No	No	5.5	No
CVE-2024-28901	Vulnerabilidad de divulgación de información de Windows Remote Access Connection Manager	Importante	No	No	5.5	No

CVE-2024-28902	Vulnerabilidad de divulgación de información de Windows Remote Access Connection Manager	Importante	No	No	5.5	No
CVE-2024-26209	Vulnerabilidad de divulgación de información del servicio del subsistema de autoridad de seguridad local de Microsoft	Importante	No	No	5.5	No
CVE-2024-26207	Vulnerabilidad de divulgación de información de Windows Remote Access Connection Manager	Importante	No	No	5.5	No
CVE-2024-26217	Vulnerabilidad de divulgación de información de Windows Remote Access Connection Manager	Importante	No	No	5.5	No
CVE-2024-28900	Vulnerabilidad de divulgación de información de Windows Remote Access Connection Manager	Importante	No	No	5.5	No
CVE-2024-26220	Vulnerabilidad de divulgación de información de puntos de acceso de Windows Mobile	Importante	No	No	5.0	No
CVE-2024-2201	**Intel**: inyección de historial de sucursales	Importante	No	No	4.7	No

CVE-2024-29056	Vulnerabilidad de elevación de privilegios de autenticación de Windows	Importante	No	No	4.3	No
CVE-2024-28922	Vulnerabilidad de omisión de la función de seguridad de arranque seguro	Importante	No	No	4.1	No
CVE-2024-29981	Vulnerabilidad de suplantación de identidad de Microsoft Edge (basado en Chromium)	Baja	No	No	4.3	No
CVE-2024-20685	Vulnerabilidad de denegación de servicio de Azure Private 5G Core	Moderada	No	No	5.9	No
CVE-2024-29992	Vulnerabilidad de divulgación de información de Azure Identity Library for .NET	Moderada	No	No	5.5	No
CVE-2024-29049	Vulnerabilidad de suplantación de identidad de Microsoft Edge (basado en Chromium) Webview2	Moderada	No	No	4.1	No
CVE-2019-3816	Mariner	Sin valor asignado	No	No	7.5	No
CVE-2019-3833	Mariner	Sin valor asignado	No	No	7.5	No
CVE-2024-3156	Chromium: implementación inapropiada en V8	Sin valor asignado				No
CVE-2024-3158	Chromium: use after free en Bookmarks	Sin valor asignado				No

CVE-2024-3159	Chromium: Acceso a memoria fuera de límites en V8	Sin valor asignado				No

4. Mitigación / Solución

Para la mitigación y la corrección de todas las vulnerabilidades, Microsoft publica las actualizaciones de seguridad pertinentes junto con sus release notes, las cuales están disponibles en Security Update Guide.

5. Referencias Adicionales

- April 2024 Security Updates.
- Security Update Guide - Microsoft.
- Zero Day initiative-The April 2024 Security Update Review.


cyber
zaintza
BASQUE CYBERSECURITY AGENCY