Basque CyberSecurity Centre

Actualización de seguridad de Microsoft-Mayo 2023

BCSC-ACTUALIZACIONES-MICROSOFT-2023-MAYO

TLP: CLEAR

www.ciberseguridad.eus

EUSKO JAURLARITZA GOBIERNO VASCO

GRUPO spri TALDEA

TABLA DE CONTENIDO

Cláusula de exención de responsabilidad

El presente documento se proporciona con el objeto de divulgar las alertas que el BCSC considera necesarias en favor de la seguridad de las organizaciones y de la ciudadanía interesada. En ningún caso el BCSC 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 BCSC 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 BCSC. 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.

Sobre el BCSC

El Centro Vasco de Ciberseguridad (Basque Cybersecurity Centre, BCSC) es la entidad designada por el Gobierno Vasco para elevar el nivel de madurez de la ciberseguridad en Euskadi.

Es una iniciativa transversal que se enmarca en la Agencia Vasca de Desarrollo Empresarial (SPRI), sociedad dependiente del Departamento de Desarrollo Económico, Sostenibilidad y Medio Ambiente del Gobierno Vasco. Así mismo, involucra a otros tres Departamentos del Gobierno Vasco: el de Seguridad, el de Gobernanza Pública y Autogobierno, y el de Educación, y a cuatro agentes de la Red Vasca de Ciencia, Tecnología e Innovación: Tecnalia, Vicomtech, Ikerlan y BCAM.

El BCSC es la entidad de referencia para el desarrollo de la ciberseguridad y de la confianza digital de ciudadanos, empresas e instituciones públicas en Euskadi, especialmente para los sectores estratégicos de la economía de la región.

La misión del BCSC es por tanto promover y desarrollar la ciberseguridad en la sociedad vasca, dinamizar la actividad empresarial de Euskadi y posibilitar la creación de un sector profesional que sea referente. En este contexto se impulsa la ejecución de proyectos de colaboración entre actores complementarios en los ámbitos de innovación tecnológica, investigación y transferencia tecnológica a la industria de fabricación avanzada y otros sectores.

Así mismo, ofrece diferentes servicios en su rol como Equipo de Repuesta a Incidentes (en adelante CERT, por sus siglas en inglés “Computer Emergency Response Team”) y trabaja en el ámbito de la Comunidad Autónoma del País Vasco para aumentar la capacidad de detección y alerta temprana de nuevas amenazas, la respuesta y análisis de incidentes de seguridad de la información, y el diseño de medidas preventivas para atender a las necesidades de la sociedad vasca. Con el fin de alcanzar estos objetivos forma parte de diferentes iniciativas orientadas a la gestión de incidentes de ciberseguridad:

FIRST Improving Security Together
TF-CSIRT Trusted Introducer
CSIRT.es

1. Resumen ejecutivo

Microsoft ha publicado las actualizaciones de seguridad del mes de mayo de 2023 en las que se corrigen 49 vulnerabilidades, siendo 6 de ellas calificadas como críticas, 33 como importantes, 1 moderada y 9 sin un valor asignado. Estas últimas corrigen problemas en el navegador Edge basado en Chromium.

Dentro de ellas existen **3 vulnerabilidades zero-day** cuyos identificadores son CVE-2023-24932, que ha sido **divulgada** y **está siendo explotada** en la última versión del software proporcionada por Microsoft, CVE-2023-29336 que también está siendo **explotada** y CVE-2023-29325 que ha sido **divulgada**.

Estas vulnerabilidades afectan a productos como Windows OLE, Microsoft SharePoint Server, Windows Bluetooth Driver, Win32k, Microsoft Excel, Microsoft Teams y Windows Kernel entre otros.

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

- 12 vulnerabilidades de ejecución remota de código.
- 9 vulnerabilidades de elevación de privilegios.
- 8 vulnerabilidades de divulgación de información.
- 5 vulnerabilidades de bypass.
- 5 vulnerabilidades de denegación de servicio.
- 1 vulnerabilidad de spoofing.
- 8 vulnerabilidades de implementación inadecuada.
- 1 vulnerabilidad de validación insuficiente de entradas.

2. Recursos afectados

Las actualizaciones de seguridad del mes de mayo de 2023 están asociadas a vulnerabilidades que afectan a los siguientes productos:

- Windows Network File System
- Windows Pragmatic General Multicast (PGM)
- Windows Lightweight Directory Access Protocol (LDAP)
- Windows Secure Socket Tunneling Protocol (SSTP)
- Windows OLE
- Microsoft SharePoint Server
- Windows Bluetooth Driver
- Win32k
- Remote Desktop Client
- Windows Backup Service
- Windows Kernel
- Microsoft Excel
- AV1 Video Extension
- SysInternals Sysmon for Windows
- Microsoft Office
- Windows SMB
- Windows NFS
- Remote Procedure Call Runtime
- Microsoft Word
- Windows Bluetooth Driver
- Windows Installer
- Windows Graphics Component
- Secure Boot
- Microsoft Teams
- Windows Bluetooth Driver
- Windows MSHTML Platform Security
- Windows NTLM Security Support Provider
- Windows iSCSI Target Service

- Windows Driver Revocation List
- Microsoft Remote Desktop app for Windows
- Visual Studio Code
- Microsoft Access
- Microsoft Edge (Chromium-based)

3. Análisis técnico

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

Las vulnerabilidades **zero-day** abordadas son:

CVE-2023-29325: vulnerabilidad de ejecución remota de código en el OLE de Windows que ha sido **divulgada.** En el caso de un ataque por correo electrónico, un atacante podría aprovechar la vulnerabilidad si envía el correo electrónico especialmente diseñado a la víctima. El aprovechamiento del fallo podría implicar que una víctima abra un correo electrónico especialmente diseñado con una versión afectada del software Microsoft Outlook o que la aplicación de Outlook de una víctima muestre una vista previa de un correo electrónico especialmente diseñado. Esto podría provocar que el atacante ejecute código remoto en la máquina de la víctima**.**

TTP

- Táctica – Initial Access TA0001
- Técnica – Phishing T1566
- Táctica – Persistence TA0003
- Técnica – Office Application Startup: Outlook Forms T1137.003

La métrica de evaluación de la vulnerabilidad se compone de:

CVSS Base: 8.1

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

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

CVE-2023-29336: vulnerabilidad de elevación de privilegios en Win32k que está siendo **explotada.** Un atacante que aprovechara esta vulnerabilidad podría obtener privilegios SYSTEM**.**

La métrica de evaluación de la vulnerabilidad se compone de:

CVSS Base: 7.8

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

- **Vector de ataque**: Local

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

CVE-2023-24932: vulnerabilidad de omisión de la característica de seguridad de arranque seguro que ha sido **divulgada** y está siendo **explotada**. Para aprovechar el fallo, un atacante que tenga acceso físico o derechos administrativos en un dispositivo de destino podría instalar una directiva de arranque manipulada, de forma que podría omitir el arranque seguro. Para aprovechar esta vulnerabilidad es necesario que un atacante ponga en peligro las credenciales de administrador del dispositivo.

TTP

- Táctica – Defense Evasion TA0005
- Técnica – Exploitation for Defense Evasion T1211

La métrica de evaluación de la vulnerabilidad se compone de:

CVSS Base: 6.7

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

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

El resto de las vulnerabilidades críticas corregidas son:

CVE-2023-24941: vulnerabilidad de ejecución remota de código en el sistema de archivos de red de Windows. Este error podría aprovecharse en la red realizando una llamada no autenticada y especialmente diseñada a un servicio de sistema de archivos de red (NFS) para desencadenar una ejecución remota de código (RCE).

TTP

- Táctica – Discovery TA0007
- Técnica – File and Directory Discovery T1083

La métrica de evaluación de la vulnerabilidad se compone de:

CVSS Base: 9.8

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

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

CVE-2023-24943: vulnerabilidad de ejecución remota de código en la multidifusión general (PGM) de Windows. Cuando el servicio Windows Message Queue Server se ejecuta en un entorno de PGM Server, un atacante podría enviar un archivo especialmente diseñado a través de la red para lograr la ejecución remota de código e intentar activar código malintencionado.

TTP

- Táctica – Lateral Movement TA0008
- Técnica – Exploitation of Remote Services T1210

La métrica de evaluación de la vulnerabilidad se compone de:

CVSS Base: 9.8

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

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

CVE-2023-28283: vulnerabilidad de ejecución remota de código en el Protocolo ligero de acceso a directorios (LDAP) en Windows. Un atacante no autenticado que aprovechara esta vulnerabilidad podría obtener la ejecución de código a través de un conjunto especialmente diseñado de llamadas LDAP para ejecutar código arbitrario en el contexto del servicio LDAP.

TTP

- Táctica – Command and Control TA0011
- Técnica – Application Layer Protocol T1071

La métrica de evaluación de la vulnerabilidad se compone de:

CVSS Base: 8.1

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

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

CVE-2023-24903: vulnerabilidad de ejecución remota de código en el Protocolo de túnel de sockets seguros (SSTP) en Windows. Para aprovechar esta vulnerabilidad, un atacante tendría que enviar un paquete SSTP malintencionado especialmente diseñado a un servidor SSTP. Esto podría resultar en la ejecución remota de código en el lado del servidor.

TTP

- Táctica – Command and Control TA0011
- Técnica – Application Layer Protocol T1071

La métrica de evaluación de la vulnerabilidad se compone de:

CVSS Base: 8.1

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

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

CVE-2023-24955: vulnerabilidad de ejecución remota de código en Microsoft SharePoint Server. En un ataque basado en red, un atacante autenticado como propietario del sitio podría ejecutar código de forma remota en SharePoint Server.

TTP

- Táctica – Defense Evasion TA0005
- Técnica – Masquerading T1036
- Táctica – Lateral Movement TA0008
- Técnica – Exploitation of Remote Services T1210

La métrica de evaluación de la vulnerabilidad se compone de:

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:

CVE	Descripción	Severidad	Divulgado	Explotado	CVSS
CVE-2023-24941	Vulnerabilidad de ejecución remota de código en el sistema de archivos de red de Windows	**Crítica**	No	No	9.8
CVE-2023-24943	Vulnerabilidad de ejecución remota de código en la multidifusión general (PGM) de Windows	**Crítica**	No	No	9.8
CVE-2023-28283	Vulnerabilidad de ejecución remota de código en el Protocolo ligero de acceso a directorios (LDAP) en Windows	**Crítica**	No	No	8.1

CVE-2023-24903	Vulnerabilidad de ejecución remota de código en el Protocolo de túnel de sockets seguros (SSTP) en Windows	**Crítica**	No	No	8.1
CVE-2023-29325	Vulnerabilidad de ejecución remota de código en el OLE de Windows	**Crítica**	Sí	No	8.1
CVE-2023-24955	Vulnerabilidad de ejecución remota de código en Microsoft SharePoint Server	**Crítica**	No	No	7.2
CVE-2023-24947	Vulnerabilidad de ejecución remota de código en el controlador Bluetooth de Windows	Importante	No	No	8.8
CVE-2023-24902	Vulnerabilidad de elevación de privilegios en Win32k	Importante	No	No	7.8
CVE-2023-24905	Vulnerabilidad de ejecución remota de código en el cliente de Escritorio remoto	Importante	No	No	7.8
CVE-2023-24946	Vulnerabilidad de elevación de privilegios en el servicio de copia de seguridad de Windows	Importante	No	No	7.8

CVE-2023-24949	Vulnerabilidad de elevación de privilegios en el kernel de Windows	Importante	No	No	7.8
CVE-2023-24953	Vulnerabilidad de ejecución remota de código en Microsoft Excel	Importante	No	No	7.8
CVE-2023-29336	Vulnerabilidad de elevación de privilegios en Win32k	Importante	No	Sí	7.8
CVE-2023-29340	Vulnerabilidad de ejecución remota de código en la extensión de vídeo AV1	Importante	No	No	7.8
CVE-2023-29341	Vulnerabilidad de ejecución remota de código en la extensión de vídeo AV1	Importante	No	No	7.8
CVE-2023-29343	Vulnerabilidad de elevación de privilegios en Sysmon para Windows	Importante	No	No	7.8
CVE-2023-29344	Vulnerabilidad de ejecución remota de código en Microsoft Office	Importante	No	No	7.8
CVE-2023-24898	Vulnerabilidad de denegación de servicio en Windows SMB	Importante	No	No	7.5
CVE-2023-24939	Vulnerabilidad de denegación de servicio en el servidor para NFS	Importante	No	No	7.5

CVE-2023-24940	Vulnerabilidad de denegación de servicio de multidifusión general (PGM) pragmática de Windows	Importante	No	No	7.5
CVE-2023-24901	Vulnerabilidad de divulgación de información del asignador de puertos NFS de Windows	Importante	No	No	7.5
CVE-2023-24942	Vulnerabilidad de denegación de servicio en tiempo de ejecución en tiempo de ejecución de llamada a procedimiento remoto	Importante	No	No	7.5
CVE-2023-29335	Vulnerabilidad de omisión de característica de seguridad en Microsoft Word	Importante	No	No	7.5
CVE-2023-29350	Vulnerabilidad de elevación de privilegios en Microsoft Edge (basado en Chromium)	Importante	No	No	7.5
CVE-2023-24948	Vulnerabilidad de elevación de privilegios en el controlador Bluetooth de Windows	Importante	No	No	7.4
CVE-2023-24904	Vulnerabilidad de elevación de privilegios en Windows Installer	Importante	No	No	7.1

CVE-2023-24899	Vulnerabilidad de elevación de privilegios en componentes gráficos de Windows	Importante	No	No	7.0
CVE-2023-24932	Vulnerabilidad de omisión de la característica de seguridad de arranque seguro	Importante	Sí	Sí	6.7
CVE-2023-24881	Vulnerabilidad de divulgación de información en Microsoft Teams	Importante	No	No	6.5
CVE-2023-24944	Vulnerabilidad de divulgación de información del controlador Bluetooth de Windows	Importante	No	No	6.5
CVE-2023-24950	Vulnerabilidad de suplantación de identidad en Microsoft SharePoint Server	Importante	No	No	6.5
CVE-2023-24954	Vulnerabilidad de divulgación de información en Microsoft SharePoint Server	Importante	No	No	6.5
CVE-2023-29324	Vulnerabilidad de omisión de característica de seguridad en la plataforma MSHTML de Windows	Importante	No	No	6.5
CVE-2023-24900	Vulnerabilidad de divulgación de información en el proveedor de soporte	Importante	No	No	5.9

	técnico de seguridad NTLM de Windows				
CVE-2023-24945	Vulnerabilidad de divulgación de información en el servicio de destino iSCSI de Windows	Importante	No	No	5.5
CVE-2023-28251	Vulnerabilidad de omisión de característica de seguridad en la lista de revocación de controladores de Windows	Importante	No	No	5.5
CVE-2023-28290	Vulnerabilidad de divulgación de información en la aplicación Escritorio remoto de Microsoft para Windows	Importante	No	No	5.3
CVE-2023-29338	Vulnerabilidad de divulgación de información en Visual Studio Code	Importante	No	No	5.0
CVE-2023-29333	Vulnerabilidad de denegación de servicio en Microsoft Access	Importante	No	No	3.3
CVE-2023-29354	Vulnerabilidad de omisión de característica de seguridad en Microsoft Edge (basado en Chromium)	Moderada	No	No	4.7
CVE-2023-2459	Chromium: Implementación inadecuada en Prompts	Sin valor asignado			

CVE-2023-2460	Chromium: Validación insuficiente de entradas que no son de confianza en extensiones	Sin valor asignado			
CVE-2023-2462	Chromium: Implementación inadecuada en Prompts	Sin valor asignado			
CVE-2023-2463	Chromium: Implementación inadecuada en modo de pantalla completa	Sin valor asignado			
CVE-2023-2464	Chromium: Implementación inadecuada en PictureInPicture	Sin valor asignado			
CVE-2023-2465	Chromium: Aplicación inadecuada en el CORS	Sin valor asignado			
CVE-2023-2466	Chromium: Implementación inadecuada en Prompts	Sin valor asignado			
CVE-2023-2467	Chromium: Implementación inadecuada en Prompts	Sin valor asignado			
CVE-2023-2468	Chromium: Implementación inadecuada en PictureInPicture	Sin valor asignado			

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

- May 2023 Security Updates.
- Security Update Guide - Microsoft.
- Zero Day initiative-The May 2023 Security Update Review.


Basque
CyberSecurity
Centre


EUSKO JAURLARITZA
GOBIERNO VASCO


GRUPO
spri
TALDEA