



Nro. Alerta:	EC-2022-60	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS <b>ALERTA DE SEGURIDAD</b>	 <p>CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS <b>ECUCERT</b></p>
TLP:	 <b>TLP:BLANCO</b>		
Fecha:	12-abril-2022	Parches de seguridad en Microsoft abril 2022	Versión 1.0

## I. DATOS GENERALES:

<b>Clase de alerta:</b>	Vulnerabilidades
<b>Tipo de incidente:</b>	Sistema o Software Abierto
<b>Nivel de riesgo:</b>	Alto

## II. ALERTA

Microsoft a través de un comunicado; dio a conocer las correcciones implementadas para un total de 145 vulnerabilidades existentes en sus productos.





**Figura 1.** Ilustración relacionada a "Patch Tuesday" de Microsoft.  
Fuente: Microsoft

## III. INTRODUCCIÓN

Microsoft, en su "martes de parches" del mes de abril dio a conocer las correcciones a 119 vulnerabilidades en diferentes productos de Microsoft y 26 vulnerabilidades asociadas directamente a Microsoft Edge basado en cromo.

- 17 Vulnerabilidades calificadas con impacto: "Desconocido".
- 3 Vulnerabilidades con gravedad "Moderado".
- 115 con gravedad "Importante".
- 10 Vulnerabilidades calificadas con impacto: "Crítico"



Nro. Alerta:	EC-2022-60	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS <b>ALERTA DE SEGURIDAD</b>	
TLP:	 <b>TLP: BLANCO</b>		
Fecha:	12-abril-2022	Parches de seguridad en Microsoft abril 2022	Versión 1.0

#### IV. VECTOR DE ATAQUE:

En al siguiente tabla, se enumera el CVE asociado y una breve descripción.


Nro.	Etiqueta	ID de CVE	Título CVE	Impacto
1	.NET Framework	<a href="#">CVE-2022-26832</a>	Vulnerabilidad de denegación de servicio de .NET Framework	Importante
2	Servicios de dominio de Active Directory	<a href="#">CVE-2022-26814</a>	Vulnerabilidad de ejecución remota de código del servidor DNS de Windows	Importante
3	Servicios de dominio de Active Directory	<a href="#">CVE-2022-26817</a>	Vulnerabilidad de ejecución remota de código del servidor DNS de Windows	Importante
4	SDK de Azure	<a href="#">CVE-2022-26907</a>	Vulnerabilidad de divulgación de información de Azure SDK para .NET	Importante
5	Recuperación del sitio de Azure	<a href="#">CVE-2022-26898</a>	Vulnerabilidad de ejecución remota de código de Azure Site Recovery	Importante
6	Recuperación del sitio de Azure	<a href="#">CVE-2022-26897</a>	Vulnerabilidad de divulgación de información de Azure Site Recovery	Importante
7	Recuperación del sitio de Azure	<a href="#">CVE-2022-26896</a>	Vulnerabilidad de divulgación de información de Azure Site Recovery	Importante
8	LDAP - Protocolo ligero de acceso a directorios	<a href="#">CVE-2022-26831</a>	Vulnerabilidad de denegación de servicio de LDAP de Windows	Importante
9	LDAP - Protocolo ligero de acceso a directorios	<a href="#">CVE-2022-26919</a>	Vulnerabilidad de ejecución remota de código LDAP de Windows	Crítico



Nro. Alerta:	EC-2022-60	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS <b>ALERTA DE SEGURIDAD</b>	
TLP:	 <b>TLP:BLANCO</b>		
Fecha:	12-abril-2022	Parches de seguridad en Microsoft abril 2022	Versión 1.0



10	Controlador Bluetooth de Microsoft	<a href="#">CVE-2022-26828</a>	Vulnerabilidad de elevación de privilegios del controlador Bluetooth de Windows	Importante
11	Dinámica de Microsoft	<a href="#">CVE-2022-23259</a>	Vulnerabilidad de ejecución remota de código de Microsoft Dynamics 365 (local)	Crítico
12	Componente de gráficos de Microsoft	<a href="#">CVE-2022-26920</a>	Vulnerabilidad de divulgación de información del componente de gráficos de Windows	Importante
13	Componente de gráficos de Microsoft	<a href="#">CVE-2022-26903</a>	Vulnerabilidad de ejecución remota de código del componente de gráficos de Windows	Importante
14	Servidor de autoridad de seguridad local de Microsoft (Isasrv)	<a href="#">CVE-2022-24493</a>	Vulnerabilidad de divulgación de información del servidor de la autoridad de seguridad local (LSA) de Microsoft	Importante
15	Excel de Microsoft Office	<a href="#">CVE-2022-24473</a>	Vulnerabilidad de ejecución remota de código de Microsoft Excel	Importante
16	Excel de Microsoft Office	<a href="#">CVE-2022-26901</a>	Vulnerabilidad de ejecución remota de código de Microsoft Excel	Importante
17	Microsoft Office SharePoint	<a href="#">CVE-2022-24472</a>	Vulnerabilidad de suplantación de identidad de Microsoft SharePoint Server	Importante
18	ALPC de Microsoft Windows	<a href="#">CVE-2022-24482</a>	Vulnerabilidad de elevación de privilegios ALPC de Windows	Importante
19	ALPC de Microsoft Windows	<a href="#">CVE-2022-24540</a>	Vulnerabilidad de elevación de privilegios ALPC de Windows	Importante



Nro. Alerta:	EC-2022-60	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS <b>ALERTA DE SEGURIDAD</b>	
TLP:	 <b>TLP:BLANCO</b>		
Fecha:	12-abril-2022	Parches de seguridad en Microsoft abril 2022	Versión 1.0



20	Biblioteca de códecs de Microsoft Windows	<a href="#">CVE-2022-24532</a>	Vulnerabilidad de ejecución remota de código de extensiones de video HEVC	Importante
21	Fundación de Microsoft Windows Media	<a href="#">CVE-2022-24495</a>	Windows Direct Show: vulnerabilidad de ejecución remota de código	Importante
22	BI de energía	<a href="#">CVE-2022-23292</a>	Vulnerabilidad de falsificación de Microsoft Power BI	Importante
23	Rol: Servidor DNS	<a href="#">CVE-2022-26815</a>	Vulnerabilidad de ejecución remota de código del servidor DNS de Windows	Importante
24	Rol: Servidor DNS	<a href="#">CVE-2022-26816</a>	Vulnerabilidad de divulgación de información del servidor DNS de Windows	Importante
25	Rol: Servidor DNS	<a href="#">CVE-2022-24536</a>	Vulnerabilidad de ejecución remota de código del servidor DNS de Windows	Importante
26	Rol: Servidor DNS	<a href="#">CVE-2022-26824</a>	Vulnerabilidad de ejecución remota de código del servidor DNS de Windows	Importante
27	Rol: Servidor DNS	<a href="#">CVE-2022-26823</a>	Vulnerabilidad de ejecución remota de código del servidor DNS de Windows	Importante
28	Rol: Servidor DNS	<a href="#">CVE-2022-26822</a>	Vulnerabilidad de ejecución remota de código del servidor DNS de Windows	Importante
29	Rol: Servidor DNS	<a href="#">CVE-2022-26829</a>	Vulnerabilidad de ejecución remota de código del servidor DNS de Windows	Importante



Nro. Alerta:	EC-2022-60	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS <b>ALERTA DE SEGURIDAD</b>	
TLP:	 <b>TLP:BLANCO</b>		
Fecha:	12-abril-2022	Parches de seguridad en Microsoft abril 2022	Versión 1.0

30	Rol: Servidor DNS	<a href="#">CVE-2022-26826</a>	Vulnerabilidad de ejecución remota de código del servidor DNS de Windows	Importante
31	Rol: Servidor DNS	<a href="#">CVE-2022-26825</a>	Vulnerabilidad de ejecución remota de código del servidor DNS de Windows	Importante
32	Rol: Servidor DNS	<a href="#">CVE-2022-26821</a>	Vulnerabilidad de ejecución remota de código del servidor DNS de Windows	Importante
33	Rol: Servidor DNS	<a href="#">CVE-2022-26820</a>	Vulnerabilidad de ejecución remota de código del servidor DNS de Windows	Importante
34	Rol: Servidor DNS	<a href="#">CVE-2022-26813</a>	Vulnerabilidad de ejecución remota de código del servidor DNS de Windows	Importante
35	Rol: Servidor DNS	<a href="#">CVE-2022-26818</a>	Vulnerabilidad de ejecución remota de código del servidor DNS de Windows	Importante
36	Rol: Servidor DNS	<a href="#">CVE-2022-26819</a>	Vulnerabilidad de ejecución remota de código del servidor DNS de Windows	Importante
37	Rol: Servidor DNS	<a href="#">CVE-2022-26811</a>	Vulnerabilidad de ejecución remota de código del servidor DNS de Windows	Importante
38	Rol: Servidor DNS	<a href="#">CVE-2022-26812</a>	Vulnerabilidad de ejecución remota de código del servidor DNS de Windows	Importante
39	Rol: Windows Hyper-V	<a href="#">CVE-2022-22008</a>	Vulnerabilidad de ejecución remota de código de Windows Hyper-V	Crítico



Nro. Alerta:	EC-2022-60	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS <b>ALERTA DE SEGURIDAD</b>	
TLP:	 <b>TLP:BLANCO</b>		
Fecha:	12-abril-2022	<b>Parches de seguridad en Microsoft abril 2022</b>	Versión 1.0

40	Rol: Windows Hyper-V	<a href="#">CVE-2022-24490</a>	Vulnerabilidad de divulgación de información de discos duros virtuales compartidos de Windows Hyper-V	Importante
41	Rol: Windows Hyper-V	<a href="#">CVE-2022-24539</a>	Vulnerabilidad de divulgación de información de discos duros virtuales compartidos de Windows Hyper-V	Importante
42	Rol: Windows Hyper-V	<a href="#">CVE-2022-26785</a>	Vulnerabilidad de divulgación de información de discos duros virtuales compartidos de Windows Hyper-V	Importante
43	Rol: Windows Hyper-V	<a href="#">CVE-2022-26783</a>	Vulnerabilidad de divulgación de información de discos duros virtuales compartidos de Windows Hyper-V	Importante
44	Rol: Windows Hyper-V	<a href="#">CVE-2022-24537</a>	Vulnerabilidad de ejecución remota de código de Windows Hyper-V	Crítico
45	Rol: Windows Hyper-V	<a href="#">CVE-2022-23268</a>	Vulnerabilidad de denegación de servicio de Windows Hyper-V	Importante
46	Rol: Windows Hyper-V	<a href="#">CVE-2022-23257</a>	Vulnerabilidad de ejecución remota de código de Windows Hyper-V	Crítico
47	Rol: Windows Hyper-V	<a href="#">CVE-2022-22009</a>	Vulnerabilidad de ejecución remota de código de Windows Hyper-V	Importante
48	Skype para empresas	<a href="#">CVE-2022-26911</a>	Vulnerabilidad de divulgación de información de Skype Empresarial	Importante
49	Skype para empresas	<a href="#">CVE-2022-26910</a>	Vulnerabilidad de suplantación de Skype Empresarial y Lync	Importante



Nro. Alerta:	EC-2022-60	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS <b>ALERTA DE SEGURIDAD</b>	
TLP:	 <b>TLP: BLANCO</b>		
Fecha:	12-abril-2022	Parches de seguridad en Microsoft abril 2022	Versión 1.0

50	Estudio visual	<a href="#">CVE-2022-24767</a>	GitHub: el desinstalador de Git para Windows es vulnerable al secuestro de DLL cuando se ejecuta con la cuenta de usuario SYSTEM	Importante
51	Estudio visual	<a href="#">CVE-2022-24765</a>	GitHub: búsqueda no controlada del directorio Git en Git para Windows	Importante
52	Estudio visual	<a href="#">CVE-2022-24513</a>	Vulnerabilidad de elevación de privilegios de Visual Studio	Importante
53	código de estudio visual	<a href="#">CVE-2022-26921</a>	Vulnerabilidad de elevación de privilegios de Visual Studio Code	Importante
54	Controlador de funciones auxiliares de Windows para WinSock	<a href="#">CVE-2022-24494</a>	Controlador de funciones auxiliares de Windows para la vulnerabilidad de elevación de privilegios de WinSock	Importante
55	Tienda de aplicaciones de Windows	<a href="#">CVE-2022-24488</a>	Vulnerabilidad de elevación de privilegios de Windows Desktop Bridge	Importante
56	Administrador de paquetes de Windows AppX	<a href="#">CVE-2022-24549</a>	Vulnerabilidad de elevación de privilegios del Administrador de paquetes de Windows AppX	Importante
57	Conmutación por error del cliente de clúster de Windows	<a href="#">CVE-2022-24489</a>	Vulnerabilidad de elevación de privilegios de conmutación por error de cliente de clúster (CCF)	Importante
58	Volumen compartido de clúster de Windows (CSV)	<a href="#">CVE-2022-24538</a>	Vulnerabilidad de denegación de servicio del volumen compartido de clúster (CSV) de Windows	Importante
59	Volumen compartido de clúster de Windows (CSV)	<a href="#">CVE-2022-26784</a>	Vulnerabilidad de denegación de servicio del volumen compartido de clúster (CSV) de Windows	Importante





Nro. Alerta:	EC-2022-60	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS <b>ALERTA DE SEGURIDAD</b>	
TLP:	 <b>TLP: BLANCO</b>		
Fecha:	12-abril-2022	<b>Parches de seguridad en Microsoft abril 2022</b>	Versión 1.0

60	Volumen compartido de clúster de Windows (CSV)	<a href="#">CVE-2022-24484</a>	Vulnerabilidad de denegación de servicio del volumen compartido de clúster (CSV) de Windows	Importante
61	Controlador del sistema de archivos de registro común de Windows	<a href="#">CVE-2022-24521</a>	Vulnerabilidad de elevación de privilegios del controlador del sistema de archivo de registro común de Windows	Importante
62	Controlador del sistema de archivos de registro común de Windows	<a href="#">CVE-2022-24481</a>	Vulnerabilidad de elevación de privilegios del controlador del sistema de archivo de registro común de Windows	Importante
63	Defensor de Windows	<a href="#">CVE-2022-24548</a>	Vulnerabilidad de denegación de servicio de Microsoft Defender	Importante
64	Biblioteca principal de DWM de Windows	<a href="#">CVE-2022-24546</a>	Vulnerabilidad de elevación de privilegios de la biblioteca principal DWM de Windows	Importante
65	Administrador de configuración de puntos finales de Windows	<a href="#">CVE-2022-24527</a>	Vulnerabilidad de elevación de privilegios del administrador de configuración de Windows Endpoint	Importante
66	Formulario de redacción de fax de Windows	<a href="#">CVE-2022-26917</a>	Vulnerabilidad de ejecución remota de código de formulario de redacción de fax de Windows	Importante
67	Formulario de redacción de fax de Windows	<a href="#">CVE-2022-26916</a>	Vulnerabilidad de ejecución remota de código de formulario de redacción de fax de Windows	Importante
68	Formulario de redacción de fax de Windows	<a href="#">CVE-2022-26918</a>	Vulnerabilidad de ejecución remota de código de formulario de redacción de fax de Windows	Importante
69	Centro de comentarios de Windows	<a href="#">CVE-2022-24479</a>	Experiencias de usuarios conectados y vulnerabilidad de elevación de privilegios de telemetría	Importante







Nro. Alerta:	EC-2022-60	<b>CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS</b>  <b>ALERTA DE SEGURIDAD</b>	
TLP:	 <b>TLP: BLANCO</b>		
Fecha:	12-abril-2022	<b>Parches de seguridad en Microsoft abril 2022</b>	Versión 1.0

70	Explorador de archivos de Windows	<a href="#">CVE-2022-26808</a>	Vulnerabilidad de elevación de privilegios del Explorador de archivos de Windows	Importante
71	Servidor de archivos de Windows	<a href="#">CVE-2022-26827</a>	Vulnerabilidad de elevación de privilegios del servicio de administración de recursos del servidor de archivos de Windows	Importante
72	Servidor de archivos de Windows	<a href="#">CVE-2022-26810</a>	Vulnerabilidad de elevación de privilegios del servicio de administración de recursos del servidor de archivos de Windows	Importante
73	instalador de ventanas	<a href="#">CVE-2022-24499</a>	Vulnerabilidad de elevación de privilegios del instalador de Windows	Importante
74	instalador de ventanas	<a href="#">CVE-2022-24530</a>	Vulnerabilidad de elevación de privilegios del instalador de Windows	Importante
75	Servicio de destino iSCSI de Windows	<a href="#">CVE-2022-24498</a>	Vulnerabilidad de divulgación de información del servicio de destino iSCSI de Windows	Importante
76	Kerberos de Windows	<a href="#">CVE-2022-24545</a>	Vulnerabilidad de ejecución remota de código Kerberos de Windows	Importante
77	Kerberos de Windows	<a href="#">CVE-2022-24486</a>	Vulnerabilidad de elevación de privilegios de Windows Kerberos	Importante
78	Kerberos de Windows	<a href="#">CVE-2022-24544</a>	Vulnerabilidad de elevación de privilegios de Windows Kerberos	Importante
79	Núcleo de Windows	<a href="#">CVE-2022-24483</a>	Vulnerabilidad de divulgación de información del kernel de Windows	Importante



Nro. Alerta:	EC-2022-60	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS <b>ALERTA DE SEGURIDAD</b>	
TLP:	 <b>TLP:BLANCO</b>		
Fecha:	12-abril-2022	<b>Parches de seguridad en Microsoft abril 2022</b>	Versión 1.0



80	Servicio de subsistema de autoridad de seguridad local de Windows	<a href="#">CVE-2022-24487</a>	Vulnerabilidad de ejecución remota de código de la autoridad de seguridad local (LSA) de Windows	Importante
81	Servicio de subsistema de autoridad de seguridad local de Windows	<a href="#">CVE-2022-24496</a>	Vulnerabilidad de elevación de privilegios de la autoridad de seguridad local (LSA)	Importante
82	Windows Media	<a href="#">CVE-2022-24547</a>	Vulnerabilidad de elevación de privilegios del receptor de Windows Digital Media	Importante
83	Sistema de archivos de red de Windows	<a href="#">CVE-2022-24491</a>	Vulnerabilidad de ejecución remota de código del sistema de archivos de red de Windows	Crítico
84	Sistema de archivos de red de Windows	<a href="#">CVE-2022-24497</a>	Vulnerabilidad de ejecución remota de código del sistema de archivos de red de Windows	Crítico
85	Windows PowerShell	<a href="#">CVE-2022-26788</a>	Vulnerabilidad de elevación de privilegios de PowerShell	Importante
86	Componentes de la cola de impresión de Windows	<a href="#">CVE-2022-26789</a>	Vulnerabilidad de elevación de privilegios de la cola de impresión de Windows	Importante
87	Componentes de la cola de impresión de Windows	<a href="#">CVE-2022-26787</a>	Vulnerabilidad de elevación de privilegios de la cola de impresión de Windows	Importante
88	Componentes de la cola de impresión de Windows	<a href="#">CVE-2022-26786</a>	Vulnerabilidad de elevación de privilegios de la cola de impresión de Windows	Importante
89	Componentes de la cola de impresión de Windows	<a href="#">CVE-2022-26796</a>	Vulnerabilidad de elevación de privilegios de la cola de impresión de Windows	Importante



Nro. Alerta:	EC-2022-60	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS <b>ALERTA DE SEGURIDAD</b>	
TLP:	 <b>TLP: BLANCO</b>		
Fecha:	12-abril-2022	<b>Parches de seguridad en Microsoft abril 2022</b>	Versión 1.0


90	Componentes de la cola de impresión de Windows	<a href="#">CVE-2022-26790</a>	Vulnerabilidad de elevación de privilegios de la cola de impresión de Windows	Importante
91	Componentes de la cola de impresión de Windows	<a href="#">CVE-2022-26803</a>	Vulnerabilidad de elevación de privilegios de la cola de impresión de Windows	Importante
92	Componentes de la cola de impresión de Windows	<a href="#">CVE-2022-26802</a>	Vulnerabilidad de elevación de privilegios de la cola de impresión de Windows	Importante
93	Componentes de la cola de impresión de Windows	<a href="#">CVE-2022-26794</a>	Vulnerabilidad de elevación de privilegios de la cola de impresión de Windows	Importante
94	Componentes de la cola de impresión de Windows	<a href="#">CVE-2022-26795</a>	Vulnerabilidad de elevación de privilegios de la cola de impresión de Windows	Importante
95	Componentes de la cola de impresión de Windows	<a href="#">CVE-2022-26797</a>	Vulnerabilidad de elevación de privilegios de la cola de impresión de Windows	Importante
96	Componentes de la cola de impresión de Windows	<a href="#">CVE-2022-26798</a>	Vulnerabilidad de elevación de privilegios de la cola de impresión de Windows	Importante
97	Componentes de la cola de impresión de Windows	<a href="#">CVE-2022-26791</a>	Vulnerabilidad de elevación de privilegios de la cola de impresión de Windows	Importante
98	Componentes de la cola de impresión de Windows	<a href="#">CVE-2022-26801</a>	Vulnerabilidad de elevación de privilegios de la cola de impresión de Windows	Importante
99	Componentes de la cola de impresión de Windows	<a href="#">CVE-2022-26793</a>	Vulnerabilidad de elevación de privilegios de la cola de impresión de Windows	Importante



Nro. Alerta:	EC-2022-60	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS <b>ALERTA DE SEGURIDAD</b>	
TLP:	 <b>TLP: BLANCO</b>		
Fecha:	12-abril-2022	Parches de seguridad en Microsoft abril 2022	Versión 1.0

100	Componentes de la cola de impresión de Windows	<a href="#">CVE-2022-26792</a>	Vulnerabilidad de elevación de privilegios de la cola de impresión de Windows	Importante
101	RDP de Windows	<a href="#">CVE-2022-24533</a>	Protocolo de escritorio remoto Vulnerabilidad de ejecución remota de código	Importante
102	Tiempo de ejecución de llamada a procedimiento remoto de Windows	<a href="#">CVE-2022-26809</a>	Tiempo de ejecución de llamada a procedimiento remoto Vulnerabilidad de ejecución remota de código	Crítico
103	Tiempo de ejecución de llamada a procedimiento remoto de Windows	<a href="#">CVE-2022-24528</a>	Tiempo de ejecución de llamada a procedimiento remoto Vulnerabilidad de ejecución remota de código	Importante
104	Tiempo de ejecución de llamada a procedimiento remoto de Windows	<a href="#">CVE-2022-24492</a>	Tiempo de ejecución de llamada a procedimiento remoto Vulnerabilidad de ejecución remota de código	Importante
105	canal de Windows	<a href="#">CVE-2022-26915</a>	Vulnerabilidad de denegación de servicio de canal seguro de Windows	Importante
106	PYME de Windows	<a href="#">CVE-2022-24485</a>	Vulnerabilidad de ejecución remota de código de enumeración de archivos Win32	Importante
107	PYME de Windows	<a href="#">CVE-2022-26830</a>	Vulnerabilidad de ejecución remota de código de DiskUsage.exe	Importante
108	PYME de Windows	<a href="#">CVE-2022-21983</a>	Vulnerabilidad de ejecución remota de código de enumeración de flujo Win32	Importante
109	PYME de Windows	<a href="#">CVE-2022-24541</a>	Vulnerabilidad de ejecución remota de código del servicio de Windows Server	Crítico



Nro. Alerta:	EC-2022-60	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS <b>ALERTA DE SEGURIDAD</b>	
TLP:	 <b>TLP:BLANCO</b>		
Fecha:	12-abril-2022	Parches de seguridad en Microsoft abril 2022	Versión 1.0

110	PYME de Windows	<a href="#">CVE-2022-24500</a>	Vulnerabilidad de ejecución remota de código SMB de Windows	Crítico
111	PYME de Windows	<a href="#">CVE-2022-24534</a>	Vulnerabilidad de ejecución remota de código de enumeración de flujo Win32	Importante
112	Servidor de telefonía de Windows	<a href="#">CVE-2022-24550</a>	Vulnerabilidad de elevación de privilegios del servidor de telefonía de Windows	Importante
113	Asistente de actualización de Windows	<a href="#">CVE-2022-24543</a>	Vulnerabilidad de ejecución remota de código del Asistente de actualización de Windows	Importante
114	Servicio de perfil de usuario de Windows	<a href="#">CVE-2022-26904</a>	Vulnerabilidad de elevación de privilegios del servicio de perfil de usuario de Windows	Importante
115	Windows Win32K	<a href="#">CVE-2022-24474</a>	Vulnerabilidad de elevación de privilegios de Windows Win32k	Importante
116	Windows Win32K	<a href="#">CVE-2022-26914</a>	Vulnerabilidad de elevación de privilegios de Win32k	Importante
117	Windows Win32K	<a href="#">CVE-2022-24542</a>	Vulnerabilidad de elevación de privilegios de Windows Win32k	Importante
118	Servicio de carpetas de trabajo de Windows	<a href="#">CVE-2022-26807</a>	Vulnerabilidad de elevación de privilegios del servicio de carpetas de trabajo de Windows	Importante
119	Proxy inverso YARP	<a href="#">CVE-2022-26924</a>	Vulnerabilidad de denegación de servicio de YARP	Importante



Nro. Alerta:	EC-2022-60	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS <b>ALERTA DE SEGURIDAD</b>	
TLP:			
Fecha:	12-abril-2022	Parches de seguridad en Microsoft abril 2022	Versión 1.0

120	Microsoft Edge (basado en cromo)	<a href="#">CVE-2022-26909</a>	Vulnerabilidad de elevación de privilegios de Microsoft Edge (basado en cromo)	Moderado
121	Microsoft Edge (basado en cromo)	<a href="#">CVE-2022-1139</a>	Chromium: CVE-2022-1139 Implementación inapropiada en API de recuperación en segundo plano	Desconocido
122	Microsoft Edge (basado en cromo)	<a href="#">CVE-2022-26912</a>	Vulnerabilidad de elevación de privilegios de Microsoft Edge (basado en cromo)	Moderado
123	Microsoft Edge (basado en cromo)	<a href="#">CVE-2022-26908</a>	Vulnerabilidad de elevación de privilegios de Microsoft Edge (basado en cromo)	Importante
124	Microsoft Edge (basado en cromo)	<a href="#">CVE-2022-1146</a>	Chromium: CVE-2022-1146 Implementación inapropiada en Resource Timing	Desconocido
125	Microsoft Edge (basado en cromo)	<a href="#">CVE-2022-26895</a>	Vulnerabilidad de elevación de privilegios de Microsoft Edge (basado en cromo)	Importante
126	Microsoft Edge (basado en cromo)	<a href="#">CVE-2022-26900</a>	Vulnerabilidad de elevación de privilegios de Microsoft Edge (basado en cromo)	Importante
127	Microsoft Edge (basado en cromo)	<a href="#">CVE-2022-26894</a>	Vulnerabilidad de elevación de privilegios de Microsoft Edge (basado en cromo)	Importante
128	Microsoft Edge (basado en cromo)	<a href="#">CVE-2022-1232</a>	Cromo: CVE-2022-1232 Confusión de tipos en V8	Desconocido
129	Microsoft Edge (basado en cromo)	<a href="#">CVE-2022-26891</a>	Vulnerabilidad de elevación de privilegios de Microsoft Edge (basado en cromo)	Importante





Nro. Alerta:	EC-2022-60	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS <b>ALERTA DE SEGURIDAD</b>	
TLP:	 <b>TLP:BLANCO</b>		
Fecha:	12-abril-2022	Parches de seguridad en Microsoft abril 2022	Versión 1.0

130	Microsoft Edge (basado en cromo)	<a href="#">CVE-2022-1125</a>	Chromium: CVE-2022-1125 Usar después de gratis en Portals	Desconocido
131	Microsoft Edge (basado en cromo)	<a href="#">CVE-2022-1136</a>	Cromo: CVE-2022-1136 Usar después de gratis en Tab Strip	Desconocido
132	Microsoft Edge (basado en cromo)	<a href="#">CVE-2022-24475</a>	Vulnerabilidad de elevación de privilegios de Microsoft Edge (basado en cromo)	Importante
133	Microsoft Edge (basado en cromo)	<a href="#">CVE-2022-1145</a>	Chromium: CVE-2022-1145 Usar después de gratis en Extensiones	Desconocido
134	Microsoft Edge (basado en cromo)	<a href="#">CVE-2022-1135</a>	Chromium: CVE-2022-1135 Usar después gratis en el carrito de compras	Desconocido
135	Microsoft Edge (basado en cromo)	<a href="#">CVE-2022-1138</a>	Chromium: CVE-2022-1138 Implementación inapropiada en Web Cursor	Desconocido
136	Microsoft Edge (basado en cromo)	<a href="#">CVE-2022-1143</a>	Chromium: CVE-2022-1143 Desbordamiento de búfer de montón en WebUI	Desconocido
137	Microsoft Edge (basado en cromo)	<a href="#">CVE-2022-24523</a>	Vulnerabilidad de suplantación de identidad de Microsoft Edge (basado en cromo)	Moderado
138	Microsoft Edge (basado en cromo)	<a href="#">CVE-2022-1137</a>	Chromium: CVE-2022-1137 Implementación inapropiada en Extensiones	Desconocido
139	Microsoft Edge (basado en cromo)	<a href="#">CVE-2022-1134</a>	Cromo: CVE-2022-1134 Confusión de tipos en V8	Desconocido



Nro. Alerta:	EC-2022-60	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS <b>ALERTA DE SEGURIDAD</b>	
TLP:	 <b>TLP: BLANCO</b>		
Fecha:	12-abril-2022	<b>Parches de seguridad en Microsoft abril 2022</b>	Versión 1.0

140	Microsoft Edge (basado en cromo)	<a href="#">CVE-2022-1127</a>	Chromium: CVE-2022-1127 Usar después de gratis en QR Code Generator	Desconocido
141	Microsoft Edge (basado en cromo)	<a href="#">CVE-2022-1128</a>	Chromium: CVE-2022-1128 Implementación inapropiada en Web Share API	Desconocido
142	Microsoft Edge (basado en cromo)	<a href="#">CVE-2022-1133</a>	Chromium: CVE-2022-1133 Usar después de gratis en WebRTC	Desconocido
143	Microsoft Edge (basado en cromo)	<a href="#">CVE-2022-1130</a>	Chromium: CVE-2022-1130 Validación insuficiente de entrada no confiable en WebOTP	Desconocido
144	Microsoft Edge (basado en cromo)	<a href="#">CVE-2022-1129</a>	Chromium: CVE-2022-1129 Implementación inapropiada en modo de pantalla completa	Desconocido
145	Microsoft Edge (basado en cromo)	<a href="#">CVE-2022-1131</a>	Chromium: CVE-2022-1131 Usar después de gratis en Cast UI	Desconocido

**Tabla 1.** Descripción CVE asociados a Microsoft abril 2022  
Fuente: Microsoft

## V. RECOMENDACIONES:

El EcuCert recomienda a su comunidad objetivo:

- Instalar las respectivas actualizaciones entregadas por el proveedor.
- Considerar la matriz de respuesta emitida por el fabricante, se sugiere revisar: <https://msrc.microsoft.com/update-guide/en-US/>



Nro. Alerta:	EC-2022-60	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS <b>ALERTA DE SEGURIDAD</b>	 <p>CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS <b>ECUCERT</b></p>
TLP:	 <p><b>TLP:BLANCO</b></p>		
Fecha:	12-abril-2022	<b>Parches de seguridad en Microsoft abril 2022</b>	Versión 1.0

## VI. REFERENCIAS:

Abrams, L. (12 de 04 de 2022). *Bleepingcomputer*. Obtenido de Bleepingcomputer:  
<https://www.bleepingcomputer.com/news/microsoft/microsoft-april-2022-patch-tuesday-fixes-119-flaws-2-zero-days/>

MICROSOFT, M. (12 de 04 de 2022). *MSRC MICROSOFT*. Obtenido de MSRC MICROSOFT:  
<https://msrc.microsoft.com/update-guide/en-US/>

