I. DATOS GENERALES:

Clase de alerta: Actualización de Seguridad

Tipo de incidente: Sistemas y/o software vulnerable

Nivel de riesgo: Medio

II. ALERTA

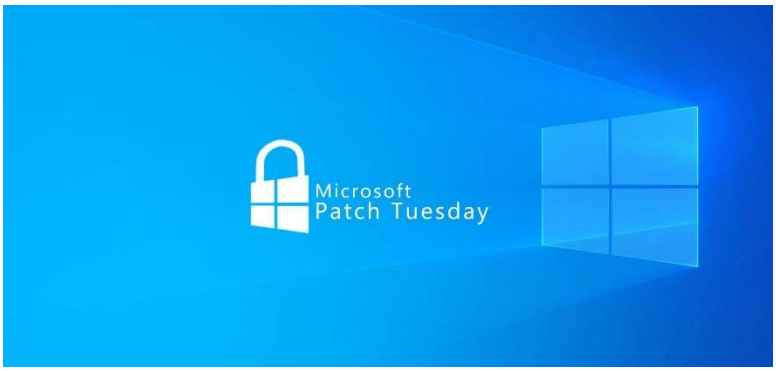

Figura 1.- martes de parches y actualizaciones de seguridad de Microsoft
Fuente: BleepingComputer

III. INTRODUCCIÓN

El 14 de febrero de 2023, Microsoft publicó parches y actualizaciones de seguridad que corrigen tres vulnerabilidades de día cero explotadas activamente y un total de 77 fallas. Nueve (9) vulnerabilidades han sido clasificadas como 'Críticas' ya que permiten la ejecución remota de código en dispositivos vulnerables.

El número de errores en cada categoría de vulnerabilidad se enumera a continuación:

- 12 Vulnerabilidades de elevación de privilegios
- 2 Vulnerabilidades de omisión de funciones de seguridad
- 38 Vulnerabilidades de ejecución remota de código
- 8 Vulnerabilidades de divulgación de información

- 10 vulnerabilidades de denegación de servicio
- 8 vulnerabilidades de suplantación de identidad

Microsoft clasifica una vulnerabilidad como de día cero si se divulga públicamente o se explota activamente sin una solución oficial disponible. Las tres vulnerabilidades de día cero explotadas activamente y corregidas en las actualizaciones de febrero son:

CVE	VULNERABILIDAD	SCORE
CVE-2023-21823	Vulnerabilidad de ejecución remota de código del componente de gráficos de Windows permite a los atacantes ejecutar comandos con privilegios de SISTEMA. La actualización de seguridad, se enviará a los usuarios a través de Microsoft Store en lugar de Windows Update.	7.5
CVE-2023-21715	Una falla en Microsoft Publisher, permitiría que un documento especialmente diseñado, puede eludir las políticas de macros de Office que bloquean archivos no confiables o maliciosos.	6.4
CVE-2023-23376	Vulnerabilidad de elevación de privilegios del controlador del sistema de archivo de registro común de Windows descubierta por Microsoft Threat Intelligence Center (MSTIC) y Microsoft Security Response Center (MSRC).	6.8

Tabla 1. Vulnerabilidades clasificadas como 'Críticas'
Fuente: BleepingComputer

A continuación la lista completa de vulnerabilidades resueltas y avisos publicados en las actualizaciones del martes de parches de febrero de 2023.

Aplicación	CVE	Título CVE	Gravedad
NET and Visual Studio	CVE-2023-21808	Vulnerabilidad de ejecución remota de código de .NET y Visual Studio	Crítico
.NET Framework	CVE-2023-21722	Vulnerabilidad de denegación de servicio de .NET Framework	Importante
3D Builder	CVE-2023-23390 CVE-2023-23377	Vulnerabilidad de ejecución remota de código de 3D Builder	Importante
	CVE-2023-23378	Vulnerabilidad de ejecución remota de código de impresión 3D	Importante
Azure App Service	CVE-2023-21777	Vulnerabilidad de elevación de privilegios Azure App Service en Azure Stack Hub	Importante
Azure Data Box Gateway	CVE-2023-21703	Vulnerabilidad de ejecución remota de código de Azure Data Box Gateway	Importante
Azure DevOps	CVE-2023-21564	Vulnerabilidad de secuencias de comandos entre sitios de Azure DevOps Server	Importante
	CVE-2023-21553	Vulnerabilidad de ejecución remota de código del servidor Azure DevOps	Importante
Azure Machine Learning	CVE-2023-23382	Vulnerabilidad de divulgación de información de la instancia informática de Azure Machine Learning	Importante
HoloLens	CVE-2019-15126	El tráfico cronometrado y diseñado específicamente puede causar errores internos (relacionados con las transiciones de estado) en un dispositivo WLAN	Desconocido
Internet Storage Name Service	CVE-2023-21699 CVE-2023-21697	Vulnerabilidad de divulgación de información del servidor del servicio de nombres de almacenamiento de Internet de Windows (iSNS)	Importante
Mariner	CVE-2022-43552	Desconocido	Desconocido
Microsoft Defender for Endpoint	CVE-2023-21809	Vulnerabilidad de omisión de la función de seguridad de punto final de Microsoft Defender	Importante
Microsoft Defender for IoT	CVE-2023-23379	Vulnerabilidad de elevación de privilegios de Microsoft Defender para IoT	Importante
Microsoft Dynamics	CVE-2023-21807 CVE-2023-21573 CVE-2023-21778 CVE-2023-21572 CVE-2023-21571 CVE-2023-21570	Vulnerabilidad de secuencias de comandos entre sitios de Microsoft Dynamics 365 (local)	Importante
Microsoft Edge (Chromium-based)	CVE-2023-23374 CVE-2023-21794	Vulnerabilidad de ejecución remota de código de Microsoft Edge (basado en cromo)	Moderado

Aplicación	CVE	Título CVE	Gravedad
	CVE-2023-21720	Vulnerabilidad de manipulación de Microsoft Edge (basado en cromo)	Bajo
Microsoft Exchange Server	CVE-2023-21710 CVE-2023-21707 CVE-2023-21706 CVE-2023-21529	Vulnerabilidad de ejecución remota de código de Microsoft Exchange Server	Importante
Microsoft Graphics Component	CVE-2023-21804 CVE-2023-21823	Vulnerabilidad de elevación de privilegios del componente de gráficos de Windows	Importante
Microsoft Office	CVE-2023-21714	Vulnerabilidad de divulgación de información de Microsoft Office	Importante
Microsoft Office OneNote	CVE-2023-21721	Vulnerabilidad de suplantación de identidad de Microsoft OneNote	Importante
Microsoft Office Publisher	CVE-2023-21715	Las características de seguridad de Microsoft Publisher evitan la vulnerabilidad	Importante
Microsoft Office SharePoint	CVE-2023-21717	Vulnerabilidad de elevación de privilegios de Microsoft SharePoint Server	Importante
Microsoft Office Word	CVE-2023-21716	Vulnerabilidad de ejecución remota de código de Microsoft Word	**Crítico**
Microsoft PostScript Printer Driver	CVE-2023-21693	Vulnerabilidad de divulgación de información del controlador de impresora PostScript de Microsoft	Importante
	CVE-2023-21801 CVE-2023-21684	Vulnerabilidad de ejecución remota de código del controlador de impresora Microsoft PostScript	Importante
Microsoft WDAC OLE DB provider for SQL	CVE-2023-21686 CVE-2023-21685 CVE-2023-21799	Proveedor Microsoft WDAC OLE DB para la vulnerabilidad de ejecución remota de código de SQL Server	Importante
Microsoft Windows Codecs Library	CVE-2023-21802	Vulnerabilidad de ejecución remota de código de Windows Media	Importante
Power BI	CVE-2023-21806	Vulnerabilidad de falsificación del servidor de informes de Power BI	Importante
SQL Server	CVE-2023-21528 CVE-2023-21713 CVE-2023-21705	Vulnerabilidad de ejecución remota de código de Microsoft SQL Server	Importante
	CVE-2023-21718	Vulnerabilidad de ejecución remota de código del controlador ODBC de Microsoft SQL	**Crítico**
	CVE-2023-21568	Servicio de integración de Microsoft SQL Server (extensión VS) Vulnerabilidad de ejecución remota de código	Importante
	CVE-2023-21704	Controlador ODBC de Microsoft para la vulnerabilidad de ejecución remota de código de SQL Server	Importante

Aplicación	CVE	Título CVE	Gravedad
Visual Studio	CVE-2023-21566	Vulnerabilidad de elevación de privilegios de Visual Studio	Importante
	CVE-2023-21815 CVE-2023-23381	Vulnerabilidad de ejecución remota de código de Visual Studio	**Crítico**
	CVE-2023-21567	Vulnerabilidad de denegación de servicio de Visual Studio	Importante
Windows Active Directory	CVE-2023-21816	Vulnerabilidad de denegación de servicio de API de servicios de dominio de Active Directory de Windows	Importante
Windows ALPC	CVE-2023-21688	Vulnerabilidad de elevación de privilegios del kernel de NT OS	Importante
Windows Common Log File System Driver	CVE-2023-23376 CVE-2023-21812	Vulnerabilidad de elevación de privilegios del controlador del sistema de archivo de registro común de Windows	Importante
Windows Cryptographic Services	CVE-2023-21813 CVE-2023-21819	Vulnerabilidad de denegación de servicio de canal seguro de Windows	Importante
Windows Distributed File System (DFS)	CVE-2023-21820	Vulnerabilidad de ejecución remota de código del sistema de archivos distribuido (DFS) de Windows	Importante
Windows Fax and Scan Service	CVE-2023-21694	Vulnerabilidad de ejecución remota de código del servicio de fax de Windows	Importante
Windows HTTP.sys	CVE-2023-21687	Vulnerabilidad de divulgación de información HTTP.sys	Importante
Windows Installer	CVE-2023-21800	Vulnerabilidad de elevación de privilegios del instalador de Windows	Importante
Windows iSCSI	CVE-2023-21803 CVE-2023-21700	Vulnerabilidad de ejecución remota de código del servicio de descubrimiento iSCSI de Windows	**Crítico**
	CVE-2023-21702 CVE-2023-21811	Vulnerabilidad de denegación de servicio del servicio iSCSI de Windows	Importante
Windows Kerberos	CVE-2023-21817	Vulnerabilidad de elevación de privilegios de Windows Kerberos	Importante
Windows MSHTML Platform	CVE-2023-21805	Vulnerabilidad de ejecución remota de código de la plataforma MSHTML de Windows	Importante
Windows ODBC Driver	CVE-2023-21797 CVE-2023-21798	Vulnerabilidad de ejecución remota de código del controlador ODBC de Microsoft	Importante
Windows Protected EAP (PEAP)	CVE-2023-21695 CVE-2023-21691 CVE-2023-21701	Vulnerabilidad de ejecución remota de código del Protocolo de autenticación extensible protegido (PEAP) de Microsoft	Importante
	CVE-2023-21692 CVE-2023-21690 CVE-2023-21689	Vulnerabilidad de ejecución remota de código del Protocolo de autenticación extensible protegido (PEAP) de Microsoft	**Crítico**

Aplicación	CVE	Título CVE	Gravedad
Windows SChannel	CVE-2023-21818	Vulnerabilidad de denegación de servicio de canal seguro de Windows	Importante
Windows Win32K	CVE-2023-21822	Vulnerabilidad de elevación de privilegios del componente de gráficos de Windows	Importante

IV. RECOMENDACIONES:

El EcuCERT recomienda a su comunidad objetivo tomar en consideración lo siguiente:

- Para actualizar un equipo personal con Windows, hacer clic en Windows Update de > de seguridad> Actualizar & Seguridad. En el área actualizaciones opcionales disponibles, seleccionar el vínculo para descargar e instalar la actualización.

- Para obtener el paquete independiente para desplegar a nivel de empresa, ingresar al sitio web del Catálogo de Microsoft Update. (https://www.catalog.update.microsoft.com/Search.aspx?q=KB5022906)

- Para obtener la actualización en WSUS manualmente, consulta el Catálogo de Microsoft Update para obtener instrucciones. (https://learn.microsoft.com/en-us/windows-server/administration/windows-server-update-services/manage/wsus-and-the-catalog-site#the-microsoft-update-catalog-site)

V. DESCARGO DE RESPONSABILIDAD.-

- La información en la presente alerta; se proporciona "tal cual" solo con fines informativos. EcuCERT no respalda ningún producto o servicio comercial, incluidos los sujetos de análisis.
- Cualquier referencia a productos, procesos o servicios comerciales específicos por marca de servicio, marca comercial, fabricante o de otro modo, no constituye ni implica respaldo, recomendación o favorecimiento por parte del EcuCERT.
- La presente alerta no debe utilizarse con fines publicitarios o de patrocinio de productos.

VI. REFERENCIAS:

ABRAMS, L. (14 de feb de 2023). *BleepingComputer*. Obtenido de https://www.bleepingcomputer.com/news/microsoft/microsoft-february-2023-patch-tuesday-fixes-3-exploited-zero-days-77-flaws/

Corporation, M. (2023). *Catálogo de Microsoft Update*. Obtenido de https://www.catalog.update.microsoft.com/Search.aspx?q=KB5022906

Corporation, M. (2023). *Catálogo de Microsoft Update*. Obtenido de https://www.catalog.update.microsoft.com/Search.aspx?q=KB5022905

Corporation, M. (2023). *Soporte técnico de Windows*. Obtenido de https://support.microsoft.com/es-es/topic/21-de-febrero-de-2023-kb5022906-compilaciones-del-so-19042-2673-19044-2673-y-19045-2673-bf72fc27-6222-4f6a-991a-f472b3f9d3fd

Corporation, M. (2023). *Soporte técnico de Windows*. Obtenido de https://support.microsoft.com/es-es/topic/versi%C3%B3n-preliminar-del-21-de-febrero-de-2023-kb5022905-compilaci%C3%B3n-del-so-22000-1641-af27b509-b478-415b-be20-3747f477f3fe