Guatemala - El Salvador - Honduras - República Dominicana

Devel
CYBERSECURITY REDEFINED

CYBER SECURITY NEWS

SECURITY OPERATIONS CENTER

MICROSOFT'S AUGUST 2023 PATCH TUESDAY CORRIGE SEIS VULNERABILIDADES CRÍTICAS Y DOS ZERO-DAYS

09/Agosto/2023

CONTENIDO

INTRODUCCIÓN

Microsoft ha parcheado un total de 74 fallas en su software como parte de las actualizaciones de Patch Tuesday de la compañía para agosto de 2023, por debajo de las voluminosas 132 vulnerabilidades que la compañía corrigió el mes pasado.

MICROSOFT'S AUGUST 2023 PATCH TUESDAY CORRIGE SEIS VULNERABILIDADES CRÍTICAS Y DOS ZERO-DAYS

A continuación, se encuentra en cuadro de identificación de la amenaza.

ID de alerta:	DSOC-CERT_2023_08_09_1
Clasificación de alerta:	Noticia
Tipo de Impacto:	Alto
TLP (Clasificación de información):	**CLEAR**
Fecha de publicación:	09/08/2023
Es día cero (0 day):	Si

RESUMEN

También son lanzadas por el gigante tecnológico dos actualizaciones de defensa en profundidad para Microsoft Office (ADV230003) y la herramienta de análisis de preparación del sistema de integridad de memoria (ADV230004).

El aviso ADV230003 sirve como una actualización sobre el problema de día cero identificado como CVE-2023-36884 (divulgado inicialmente en el parche del martes de julio de 2023). La segunda preocupación de día cero abordada por el martes de parches de agosto de 2023 está etiquetada como CVE-2023-38180.

Los siguientes tipos de vulnerabilidades se incluyen en el martes de parches de agosto:

- 23 vulnerabilidades de ejecución remota de código (RCE)
- 18 vulnerabilidades de elevación de privilegios (EoP)
- 12 vulnerabilidades de suplantación de identidad
- 9 vulnerabilidades de divulgación de información

- 8 vulnerabilidades de denegación de servicio (DoS)
- 4 vulnerabilidades de omisión de características de seguridad

VULNERABILIDADES DE DÍA CERO BAJO EXPLOTACIÓN ACTIVA: CVE-2023-36884 Y CVE-2023-38180

CVE-2023-36884 (puntuación CVSS: 7,5): la vulnerabilidad implica la explotación de Microsoft Office y su mecanismo de defensa. Originalmente se pensó que era una vulnerabilidad de ejecución remota de código y se abordó en Microsoft July 2023 Patch Tuesday. Sin embargo, más tarde se clasificó como una omisión de función de seguridad.
CVE-2023-36884 permite a los atacantes crear documentos especializados de Microsoft Office para eludir la función de seguridad Mark of the Web (MoTW), abriendo archivos sin advertencias y permitiendo la ejecución remota de código. El grupo RomCom, ahora llamado "Underground", explotó activamente esta vulnerabilidad.

CVE-2023-38180 (puntuación CVSS: 7,5): esta vulnerabilidad se dirige a aplicaciones .NET y Visual Studio, lo que permite a los atacantes lanzar ataques de denegación de servicio distribuido (DDoS). Si bien los detalles específicos sobre la explotación siguen sin revelarse, su potencial de impacto generalizado es preocupante. Estas vulnerabilidades de día cero subrayan la urgencia de aplicar actualizaciones rápidamente y la importancia de la detección avanzada de amenazas

VULNERABILIDADES CRÍTICAS DEL MARTES DE PARCHES DE AGOSTO DE 2023

Un enfoque particular recae en vulnerabilidades como CVE-2023-35385, CVE-2023-36910 y CVE-2023-36911, que afectan a Microsoft Message Queuing. Estas vulnerabilidades de ejecución remota de código resaltan la importancia de proteger los servicios esenciales que los atacantes podrían explotar para infiltrarse en los sistemas.

CVE-2023-35385 (puntuación CVSS: 9,8): si esta vulnerabilidad se aprovecha con éxito, un atacante no autorizado podría ejecutar código de forma remota en el servidor de destino.

CVE-2023-36911 (puntuación CVSS: 9,8): la vulnerabilidad permite que un atacante no autenticado ejecute código de forma remota en el servidor de destino.

CVE-2023-36910 (puntuación CVSS: 9,8): un atacante podría aprovechar esta vulnerabilidad enviando un paquete MSMQ malicioso especialmente diseñado a un servidor MSMQ, lo que le permite ejecutar código remoto del lado del servidor.

CVE-2023-29328 y CVE-2023-29330 (puntaje CVSS: 8.8): un atacante podría manipular a una víctima para que participe en una reunión de Teams para lograr la ejecución remota de código. Esto permite que el atacante acceda a los datos de la víctima, lo que les permite verlos y modificarlos. Además, este exploit tiene el potencial de interrumpir la máquina del cliente, lo que genera períodos de inactividad.

CVE-2023-36895 (puntaje CVSS: 7.8): la vulnerabilidad permite la ejecución remota de código dentro de Microsoft Outlook. Según el aviso, la actualización de seguridad aún no está disponible para Microsoft Office 2019 para Mac y Microsoft Office LTSC para Mac 2021. Microsoft aclara que se notificará a los clientes sobre la actualización a través del aviso.

Le recomendamos encarecidamente que aplique los parches lo antes posible para proteger su entorno y mejorar su postura de seguridad. Puede encontrar más información sobre las vulnerabilidades cubiertas en esta actualización en la Nota de lanzamiento de Microsoft.

RECOMENDACIONES

- Se recomienda la actualización inmediata de los sistemas mediante Windows Update.
- El proveedor recomienda ajustes, configuraciones comunes o bien buenas prácticas generales.

NOTICIA COMPLETA

https://devel.group/blog/microsofts-august-2023-patch-tuesday-corrige-seis-vulnerabilidades-criticas-y-dos-dia-cero/

CONTACTOS DE SOPORTE

Correo electrónico: cert@develsecurity.com

Teléfonos directos:

Guatemala: +(502) 2307 5757

El Salvador: +(503) 2249 4252

Honduras: +(504) 2283 5904

República Dominicana: +1 829 734 2040

WhatsApp: +(502) 5124 9536

Sitio Web: https://www.devel.group/reporta-un-incidente