Guatemala - El Salvador - Honduras - República Dominicana

Devel
CYBERSECURITY REDEFINED

CYBER SECURITY NEWS

SECURITY OPERATIONS CENTER

MICROSOFT LIBERA ACTUALIZACIONES PARA VULNERABILIDADES CRITICAS

05 / Abril / 2023

CONTENIDO

INTRODUCCIÓN

Microsoft ha lanzado un nuevo listado de actualizaciones para Windows, lo cual permitirá a la corrección de 98 vulnerabilidades de las cuales 7 se consideran actualmente como críticas. Dichas actualizaciones también incluyen la corrección de una vulnerabilidad ZERO-DAY.

ACTUALIZACIONES DE SEGURIDAD PARA MICROSOFT WINDOWS

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

ID de alerta:	DSOC-CERT_2023_04_13_2
Clasificación de alerta:	Noticia
Tipo de Impacto:	Alta
TLP (Clasificación de información):	**CLEAR**
Fecha de publicación:	13/04/2023
Es día cero (0 day):	Sí

RESUMEN

Como parte de sus actualizaciones de Abril, Windows ha lanzado nuevas actualizaciones que pretende corregir varias vulnerabilidades en Windows, concretamente 98 vulnerabilidades entre las cuales 7 han sido catalogadas críticas y requieren actualización inmediata. De estas anteriores también se ha liberado actualización para la corrección de una vulnerabilidad ZERO-DAY (CVE-2023-28253).

Con estas actualizaciones se busca corregir las distintas vulnerabilidades a continuación expuestas:

- 20 vulnerabilidades de elevación de privilegios.
- 8 vulnerabilidades de omisión de características de seguridad.
- 45 vulnerabilidades de ejecución remota de código.
- 10 vulnerabilidades de divulgación de información.
- 9 vulnerabilidades de denegación de servicios.
- 6 vulnerabilidades de suplantación

VULNERABILIDAD ZERO-DAY

Como se mencionaba con anterioridad, el listado de actualizaciones incluye la corrección de una vulnerabilidad ZERO-DAY:

CVE-2023-28252 (7.8): Vulnerabilidad de elevación de privilegios del controlados del sistema de archivo de registro común de Windows.

El cual afecta a todas las versiones soportadas de servidores y clientes Windows y puede ser explotado por atacantes locales en ataques de baja complejidad sin interacción del usuario.
Permitiendo a los actores obtener privilegios de SYSTEM y comprometer completamente los sistemas Windows objetivo.

VULNERABILIDADES CRITICAS

QueueJumper

- CVE-2023-21554: Vulnerabilidad de ejecución remota de cola de mensajería de Microsoft (MSMQ)
    - Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Código de ejecución remota sin autorización mediante puerto 1801 (TCP), el atacante envía un paquete de MSMQ especialmente elaborado hacia el puerto 1801/TCP lo que resulta en el Código de ejecución remota en el lado del servidor. Esto es posible ya que MSMQ es un “middleware” en las cuales ciertos softwares populares se basan. De manera que cuando se instala el software. El servicio MSMQ se activa en Windows inclusive sin el conocimiento del usuario.

De la mano de la vulnerabilidad encontrada en Cola de Mensajería de Microsoft (MSMQ) se denotan las siguientes vulnerabilidades críticas:

- CVE-2023-21769: Vulnerabilidad de denegación de servicios en Cola de Mensajería de Microsoft (MSMQ)
    - Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
- CVE-2023-28302: Vulnerabilidad de denegación de servicios remoto no autenticado a nivel de Kernel (Windows BSOD)
    - Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

- CVE-2023-28250: Vulnerabilidad de servicios de Cola de Mensajería de Microsoft (MSMQ) de código de ejecución remota. El atacante envía un archivo especialmente diseñado por medio de

la red lo que permite la ejecución remota de código para posteriormente desencadenar código malicioso en el equipo afectado.

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

- CVE-2023-28219: Vulnerabilidad de código de ejecución remota del Protocolo de Túnel de Capa 2 (L2TP). Un atacante no autenticado envía una solicitud de conexión especialmente diseñada a un servidor RAS, lo cual podría conducir a la ejecución remota de código (RCE) en la máquina del servidor RAS.
    - Vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H

- CVE-2023-28232: Vulnerabilidad de código de ejecución remota del Protocolo de Túnel Punto a punto de Windows (PPTP). El atacante puede aprovechar la vulnerabilidad en el momento que un usuario conecta un cliente de Windows a un servidor Malicioso.
    - Vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H

VULNERABILIDADES POR CORREGIR

A continuación, se presenta el listado de vulnerabilidades a parchear, seguido de su puntuación CVSS:

- CVE-2023-28260 –7.8/10.0
- CVE-2023-28300 –7.5/10.0
- CVE-2023-28227 –7.5/10.0
- CVE-2023-28309 –7.6/10.0
- CVE-2023-24912 –7.8/10.0
- CVE-2023-21769 –7.5/10.0
- CVE-2023-21554 –9.8/10.0
- CVE-2023-28287 – 7.8/10.0
- CVE-2023-28311 –7.8/10.0
- CVE-2023-28243 –8.8/10.0
- CVE-2023-24927 –8.8/10.0
- CVE-2023-24925 –8.8/10.0
- CVE-2023-24924 –8.8/10.0
- CVE-2023-24885 –8.8/10.0
- CVE-2023-24928 –8.8/10.0
- CVE-2023-24884 –8.8/10.0
- CVE-2023-24926 –8.8/10.0
- CVE-2023-24929 –8.8/10.0
- CVE-2023-24887 –8.8/10.0
- CVE-2023-24886 –8.8/10.0

- CVE-2023-28275 –8.8/10.0
- CVE-2023-28254 –7.2/10.0
- CVE-2023-23384 –7.3/10.0
- CVE-2023-23375 –7.8/10.0
- CVE-2023-28304 –7.8/10.0
- CVE-2023-28262 –7.8/10.0
- CVE-2023-28296 – 8.4/10.0
- CVE-2023-24893 –7.8/10.0
- CVE-2023-28302 –7.5/10.0
- CVE-2023-28236 –7.8/10.0
- CVE-2023-28216 –7.0/10.0
- CVE-2023-28218 –7.0/10.0
- CVE-2023-28273 –7.0/10.0
- CVE-2023-28229 –7.0/10.0
- CVE-2023-28252 –7.8/10.0
- CVE-2023-28231 –8.8/10.0
- CVE-2023-28221 –7.0/10.0
- CVE-2023-28238 –7.5/10.0
- CVE-2023-28244 –8.1/10.0
- CVE-2023-28248 –7.8/10.0
- CVE-2023-28222 –7.1/10.0
- CVE-2023-28272 –7.8/10.0
- CVE-2023-28293 –7.8/10.0
- CVE-2023-28237 –7.8/10.0
- CVE-2023-28219 –8.1/10.0
- CVE-2023-28220 –8.1/10.0
- CVE-2023-28268 –8.1/10.0
- CVE-2023-28217 –7.1/10.0
- CVE-2023-28247 –7.5/10.0
- CVE-2023-28240 –8.8/10.0
- CVE-2023-28225 –7.8/10.0
- CVE-2023-28250 –9.8/10.0
- CVE-2023-28224 –7.1/10.0
- CVE-2023-28232 –7.5/10.0
- CVE-2023-28291 –8.4/10.0
- CVE-2023-28292 –7.8/10.0
- CVE-2023-28246 –7.8/10.0
- CVE-2023-21727 –8.8/10.0
- CVE-2023-28297 –8.8/10.0
- CVE-2023-24931 –7.5/10.0
- CVE-2023-28233 –7.5/10.0
- CVE-2023-28241 –7.5/10.0

- CVE-2023-28234 –7.5/10.0
- CVE-2023-28274 –7.8/10.0
- CVE-2023-24914 –7.0/10.0

RECOMENDACIÓN

- Se recomienda la actualización inmediata de los sistemas mediante **Windows Update**.
- El proveedor recomienda ajustes, configuraciones comunes o bien buenas prácticas generales.
- chequear si el servicio llamado "Message Queuing" y el puerto TCP 1801 se encuentra enlistado en la máquina.

NOTICIA COMPLETA

https://devel.group/blog/actualizaciones-de-seguridad-para-microsoft-windows-abril-2023/

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