El primer paquete de correcciones del martes de parches enviadas por Microsoft para 2023 abordaron un total de 98 vulnerabilidades de seguridad, incluyendo una falla que, según la compañía, se está explotando activamente en la naturaleza.

11 de los 98 problemas están clasificados como críticos, 87 como importantes en gravedad y una de las vulnerabilidades figura como conocida públicamente en el momento del lanzamiento. De forma separada, se espera que el fabricante de Windows publique actualizaciones para su navegador Edge basado en Chromium.

La vulnerabilidad que está bajo ataque se relaciona con CVE-2023-21674 (puntaje CVSS: 8.8), una vulnerabilidad de escalada de privilegios en Windows Advanced Local Procedure Call (ALPC), que podría ser explotada por un hacker para obtener permisos de SISTEMA.

«Esta vulnerabilidad podría conducir a una escape de la sandbox del navegador», dijo Microsoft en un aviso, acreditando a los investigadores de Avast, Jan Vojtěšek, Milánek y Przemek Gmerek por informar el error.

Aunque los detalles de la vulnerabilidad siguen en secreto, una explotación exitosa requiere que un atacante ya haya obtenido una infección inicial en el host. También es probable que la vulnerabilidad se combine con un error presente en el navegador web para salir de la zona de pruebas y obtener privilegios elevados.

> *«Una vez que se haya hecho el punto de apoyo inicial, los atacantes buscarán moverse a través de una red u obtener niveles de acceso más altos adicionales y este tipo de vulnerabilidades de escalada de privilegios son una parte clave del libro de jugadas de ese atacante»,* dijo Kev Breen, director de investigación de amenazas cibernéticas en Immersive Labs.

De este modo, las posibilidades de que una cadena de explotación como esta se emplee de forma generalizada son limitadas debido a la función de actualización automática usada para parchear los navegadores, dijo Satnam Narang, ingeniero de investigación senior de Tenable.

Además, la Agencia de Seguridad de Infraestructura y Ciberseguridad de Estados Unidos (CISA), agregó la vulnerabilidad a su Catálogo de Vulnerabilidades Explotadas Conocidas (KEV), instando a las agencias federales a aplicar parches antes del 31 de enero de 2023.

CVE-2023-21674 es la cuarta vulnerabilidad de este tipo identificada en ALPC, una función de comunicación entre procesos (IPC) proporcionada por el kernel de Microsoft Windows, después de CVE-2022-41045, CVE-2022-41093 y CVE-2022-41100 (puntajes CVSS: 7.8), las últimas tres de las cuales se conectaron en noviembre de 2022.

Otras dos vulnerabilidades de escalada de privilegios identificadas como de alta prioridad afectan a Microsoft Exchange Server (CVE-2023-21763 y CVE-2023-21764, puntuaciones CVSS: 7.8), que se derivan de un parche incompleto para CVE-2022-41123, según Qualys.

> *«Un atacante podría ejecutar código con privilegios de nivel de SISTEMA al explotar una ruta de archivo codificada»,* dijo Saeed Abbasi, gerente de investigación de vulnerabilidades y amenazas en Qualys.

Microsoft también corrigió una omisión de la función de seguridad en SharePoint Server (CVE-2023-21743, puntaje CVSS: 5.3) que podría permitir que un hacker no autenticado eluda la autenticación y realice una conexión anónima. La compañía dijo que *«los clientes también deben activar una acción de actualización de SharePoint incluida en esta actualización para proteger su granja de SharePoint».*

La actualización de enero corrige aún más una serie de vulnerabilidades de escalada de privilegios, incluida una en el Administrador de Credenciales de Windows (CVE-2023-21726, puntuación CVSS: 7.8) y tres que afectan el componente Print Spooler (CVE-2023-21678, CVE-2023-21760 y CVE-2023-21765).

A la Agencia de Seguridad Nacional de Estados Unidos (NSA) se le atribuye el informe de CVE-2023-21678. En total, 39 de las vulnerabilidades que Microsoft cerró en su última actualización permiten la elevación de privilegios.

En la lista también se encuentra CVE-2023-21549 (puntuación CVSS: 8.8), una vulnerabilidad de elevación de privilegios conocida públicamente en el servicio de testigo SMB de Windows y otra instancia de omisión de características de seguridad que afecta a BitLocker (CVE-2023-21563, puntuación CVSS: 6.8).

> *«Un atacante exitoso podría eludir la función de cifrado del dispositivo BitLocker en el dispositivo de almacenamiento del sistema. Un atacante con acceso físico al objetivo podría explotar esta vulnerabilidad para obtener acceso a datos cifrados»,* dijo Microsoft.

Finalmente, Redmond revisó su guía sobre el uso malicioso de controladores firmados (llamado Traiga su propio controlador vulnerable) para incluir una lista de bloqueo actualizada publicada como parte de las actualizaciones de seguridad de Windows el 10 de enero de 2023.

El martes, CISA también agregó CVE-2022-41080, una vulnerabilidad de escalada de privilegios de Exchange Server, al catálogo de KEV después de informes acerca de que la vulnerabilidad se está encadenando junto con CVE-2022-41082 para lograr la ejecución remota de código en sistemas vulnerables.

El exploit, cuyo nombre en código es OWASSRF por CrowdStrike, ha sido aprovechado por los atacantes del ransomware Play para violar los entornos de destino. Microsoft corrigió los defectos en noviembre de 2022.

Las actualizaciones del martes de parches también llegan cuando Windows 7, Windows 8.1 y Windows RT llegaron al final del soporte el 10 de enero de 2023. Microsoft dijo que no ofrecerá un programa de actualización de seguridad extendida (ESU) para Windows 8.1, sino que instará a los usuarios a actualizar a Windows 11.

> *«Seguir usando Windows 8.1 después del 10 de enero de 2023 puede aumentar la*

> *exposición de una organización a los riesgos de seguridad o afectar su capacidad para cumplir con las obligaciones de cumplimiento»,* dijo la compañía.