Boletín de Ciberseguridad N°64

Fecha de publicación: 15/08/2023

Mes de agosto

26/07/2023 – 15/08/2023

Datasec

BOLETÍN DE CIBERSEGURIDAD

Indice

Introducción

Por medio de este boletín informativo estaremos destacando de forma quincenal, las noticias más relevantes en el ámbito de la ciberseguridad a nivel regional e internacional.

Las principales categorías de información son: vulnerabilidades tecnológicas, fraudes activos, amenazas por medios informáticos nuevos, así como recomendaciones específicas de prevención.

La publicación de dichas noticias dependerá de la importancia y calidad informativa de las mismas.

A su vez se incluyen referencias técnicas y de gestión a los efectos de reducir los riesgos con anticipación y adecuada planificación.

En esta primera quincena del mes de agosto se destacan 5 noticias de relevancia: 2 sobre vulnerabilidades tecnológicas, y 3 de prevención.

Aquellas noticias a tener especial recaudo son las siguientes:

CISA agrega una vulnerabilidad de Microsoft .NET

CISA agregó una falla de seguridad recientemente parcheada en los productos .NET y Visual Studio de Microsoft a su catálogo de Vulnerabilidades Explotadas Conocidas, citando evidencia de explotación activa.

Se descubre una nueva vulnerabilidad de alta gravedad

Se ha descubierto una nueva falla de seguridad de alta gravedad en el software de administración de impresión PaperCut para Windows que podría resultar en la ejecución remota de código en circunstancias específicas.

Microsoft lanza parches para 74 nuevas vulnerabilidades

Microsoft ha reparado 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 solucionó el mes pasado.

Vulnerabilidad Crítica

	CISA agrega una vulnerabilidad de Microsoft .NET	CRÍTICO

Descripción

CISA agregó una falla de seguridad recientemente parcheada en los productos .NET y Visual Studio de Microsoft a su catálogo de Vulnerabilidades Explotadas Conocidas, citando evidencia de explotación activa.

Estado

Registrado como CVE-2023-38180 (puntuación CVSS: 7,5), la falla de alta gravedad se relaciona con un caso de denegación de servicio (DoS) que afecta a .NET y Visual Studio.

Microsoft lo abordó como parte de sus actualizaciones del martes de parches de agosto de 2023 enviadas a principios de esta semana, etiquetándolo con una evaluación de "Explotación más probable".

Si bien los detalles exactos sobre la naturaleza de la explotación no están claros, el fabricante de Windows ha reconocido la existencia de una prueba de concepto (PoC) en su aviso. También dijo que los ataques que aprovechan la falla se pueden realizar sin ningún privilegio adicional o interacción del usuario.

Las versiones afectadas del software incluyen ASP.NET Core 2.1, .NET 6.0, .NET 7.0, Microsoft Visual Studio 2022 versión 17.2, Microsoft Visual Studio 2022 versión 17.4 y Microsoft Visual Studio 2022 versión 17.6.

Remediación / Referencias

Se recomienda a las agencias del Poder Ejecutivo Civil Federal que apliquen las correcciones proporcionadas por los proveedores para la vulnerabilidad.

https://www.cisa.gov/news-events/alerts/2023/08/09/cisa-adds-one-known-exploited-vulnerability-catalog

PaperCut	**Se descubre una nueva vulnerabilidad de alta gravedad**	CRÍTICO

Descripción

Se ha descubierto una nueva falla de seguridad de alta gravedad en el software de administración de impresión PaperCut para Windows que podría resultar en la ejecución remota de código en circunstancias específicas.

Estado

Registrado como CVE-2023-39143 (puntuación CVSS: 8.4), la falla afecta a PaperCut NG/MF antes de la versión 22.1.3. Se ha descrito como una combinación de vulnerabilidad de transferencia de ruta y carga de archivos.

La firma de ciberseguridad dijo que la carga de archivos que conducen a la ejecución remota de código es posible cuando la configuración de integración de dispositivos externos está habilitada, que está activada de forma predeterminada en algunas instalaciones de PaperCut.

A principios de abril, otra vulnerabilidad de ejecución remota de código en el mismo producto (CVE-2023-27350, puntaje CVSS: 9.8) y una falla de divulgación de información (CVE-2023–27351) fueron objeto de una explotación generalizada en la naturaleza para entregar Cobalt Strike y ransomware . . Los actores del estado-nación iraní también fueron vistos abusando de los errores para obtener acceso inicial a las redes de destino.

Remediación / Referencias

PaperCut remedió en la versión 22.1.3 una falla de seguridad que podría permitir que un atacante no autenticado con acceso directo a la IP del servidor cargue archivos arbitrarios en un directorio de destino, lo que lleva a una posible denegación de servicio (CVE-2023-3486, CVSS puntuación: 7,4). A Tenable se le atribuye el descubrimiento y la notificación del problema.

Por mayor información acceder a:

https://nvd.nist.gov/vuln/detail/CVE-2023-39143

Prevención

Surge nuevo malware Statc Stealer

PREVENCIÓN

Descripción

Se ha encontrado una nueva cepa de malware de información llamada Statc Stealer que infecta dispositivos que ejecutan Microsoft Windows para desviar información personal y de pago confidencial.

Estado

Escrito en C++, el ladrón malicioso se abre paso en los sistemas de las víctimas cuando se engaña a las víctimas potenciales para que hagan clic en anuncios aparentemente inocuos, y el ladrón imita un formato de archivo de video MP4 en navegadores web como Google Chrome.

La carga útil de la primera etapa, al colocar y ejecutar un instalador de PDF señuelo, también implementa sigilosamente un binario de descarga que procede a recuperar el malware ladrón de un servidor remoto a través de un script de PowerShell.

El ladrón presenta controles sofisticados para inhibir la detección de sandbox y el análisis de ingeniería inversa, y establece conexiones con un servidor de comando y control (C&C) para filtrar los datos recopilados mediante HTTPS.

Uno de los antianálisis incluye una comparación de los nombres de archivo para inspeccionar cualquier discrepancia y detener su ejecución, si se encuentra. Los navegadores web objetivo incluyen Google Chrome, Microsoft Edge, Mozilla Firefox, Brave, Opera y Yandex Browser.

Remediación / Referencias

Se recomienda la versión actualizada ya que incluye funciones como la recopilación de datos de Signal Messenger y la limpieza de la detección de Defender.

Por mayor información acceder a:

https://www.zscaler.es/blogs/security-research/statc-stealer-decoding-elusive-malware-threat

Microsoft lanza parches para 74 nuevas vulnerabilidades

PREVENCIÓN

Descripción

Microsoft ha reparado 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 solucionó el mes pasado.

Estado

Esto comprende seis vulnerabilidades críticas, 67 importantes y una de gravedad moderada. Junto con las mejoras de seguridad, se lanzaron dos actualizaciones de defensa en profundidad para Microsoft Office (ADV230003) y la herramienta de escaneo Memory Integrity System Readiness Scan Tool (ADV230004).

Las actualizaciones también se suman a los 30 problemas abordados por Microsoft en su navegador Edge basado en Chromium desde la edición Patch Tuesday del mes pasado y una falla de canal lateral que afecta a ciertos modelos de procesador ofrecidos por AMD (CVE-2023-20569 o Inception).

ADV230003 se refiere a una falla de seguridad ya conocida rastreada como CVE-2023-36884, una vulnerabilidad de ejecución remota de código en Office y Windows HTML que ha sido explotada activamente por el actor de amenazas RomCom vinculado a Rusia en ataques dirigidos a Ucrania, así como a objetivos pro-Ucrania en Europa del Este y América del Norte.

Otras tres vulnerabilidades destacadas son CVE-2023-35388, CVE-2023-38182 (puntuación CVSS: 8,0) y CVE-2023-38185 (puntuación CVSS: 8,8) – fallas de ejecución remota de código en Exchange Server – las dos primeras de las cuales han sido etiquetados con una evaluación de "explotación más probable".

Microsoft reconoció además la disponibilidad de un exploit de prueba de concepto (PoC) para una vulnerabilidad DoS en .NET y Visual Studio (CVE-2023-38180 , puntaje CVSS: 7.5), y señaló que el "código o técnica no es funcional en todas las situaciones y puede requerir una modificación sustancial por parte de un atacante experto".

Remediación / Referencias

La actualización también incluye parches para cinco fallas de escalada de privilegios en el kernel de Windows (CVE-2023-35359 , CVE-2023-35380 , CVE-2023-35382 , CVE-2023-35386

y CVE-2023-38154 , puntajes CVSS) : 7.8) que podría ser armado por un actor de amenazas con acceso local a la máquina de destino para obtener privilegios de SISTEMA.

Por mayor información acceder a:

https://learn.microsoft.com/es-es/microsoft-365/security/defender-vulnerability-management/tvm-remediation?view=o365-worldwide

Descripción

Microsoft reveló el viernes que ha abordado una falla de seguridad crítica que afecta a Power Platform, pero no antes de que fuera criticado por no haber actuado rápidamente al respecto.

Estado

La compañía señaló además que no se requiere ninguna acción del cliente y que no encontró evidencia de explotación activa de la vulnerabilidad en la naturaleza.

La firma de ciberseguridad dijo que la falla surge como resultado de un control de acceso insuficiente a los hosts de Azure Functions, lo que lleva a un escenario en el que un actor de amenazas podría interceptar ID y secretos de clientes de OAuth, así como otras formas de autenticación.

Se dice que Microsoft emitió una solución inicial el 7 de junio de 2023, pero no fue hasta el 2 de agosto de 2023 que la vulnerabilidad se solucionó por completo.

La demora de meses en reparar la falla atrajo el escrutinio del CEO de Tenable, Amit Yoran, quien criticó al fabricante de Windows por ser "extremadamente irresponsable, si no descaradamente negligente".

Remediación / Referencias

Sigue un extenso proceso de investigación e implementación de correcciones.

Por mayor información acceder a: https://windows.atsit.in/es/16096/

Conclusiones

Las noticias contenidas en este boletín advierten sobre las nuevas modalidades y distintos ataques utilizados por ciberdelincuentes para alterar documentación digitalizada, falsificando y afectando la autenticidad de los mismos.

Recomendamos estar atentos y mantenerse informados respecto al phishing y a otras modalidades de ingeniería social, ya que se observa un incremento constante de intentos de engañar a las víctimas, mediante correos que buscan suplantar instituciones de manera ilegítima para robar y manipular información sensible de los clientes.

Seguimos viendo la importancia de estar atentos a las nuevas amenazas emergentes y a la importancia de aplicar actualizaciones.

En este último tiempo la evolución de las amenazas de software se incrementa mes a mes. Recomendamos seguir midiendo nuestros estados de ciberseguridad en los accesos críticos del negocio y las conexiones laterales que puedan surgir de exponer la información sobre los diferentes canales de datos.

Desde el equipo de Datasec seguimos protegiendo la seguridad de nuestros clientes, socios y colaboradores.

¡Sigan protegiéndose!