Boletín de Ciberseguridad

Fecha de Publicación
10/04/2023 - N.º 56

Mes de Abril
27/03/2023 - 10/04/2023

Datasec

Índice

Introducción....2
CISA advierte sobre 5 fallas de seguridad explotadas activamente....3
Nueva falla de seguridad del protocolo Wi-Fi que afecta a dispositivos Linux, Android e iOS..4
El nuevo malware MacStealer macOS roba datos y contraseñas del llavero de iCloud....5
Descubren una falla crítica de ejecución remota de código en la biblioteca Sandbox de vm2.6
Aplicación de escritorio 3CX utilizada en un ataque a la cadena de suministro....7
Apple lanza actualizaciones para abordar fallas de día cero en iOS, iPadOS, macOS y Safari..9
Microsoft corrige una nueva vulnerabilidad de Azure AD....10
Conclusiones....12

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 abril se destacan 5 noticias de relevancia: cinco de vulnerabilidades y dos de prevención.

Aquellas noticias a tener especial recaudo son las siguientes:

CISA advierte sobre 5 fallas de seguridad explotadas activamente

Se agregaron cinco fallas de seguridad al catálogo de Vulnerabilidades Explotadas Conocidas (KEV), citando evidencia de explotación activa en la naturaleza.

El nuevo malware MacStealer macOS roba datos y contraseñas del llavero de iCloud

Un nuevo malware que roba información se ha fijado en el sistema operativo macOS de Apple para desviar información confidencial de los dispositivos comprometidos.

Microsoft corrige una nueva vulnerabilidad de Azure AD

Microsoft solucionó un problema de configuración incorrecta que afectaba el servicio de gestión de acceso e identidad de Azure Active Directory (AAD) que exponía varias aplicaciones de "alto impacto" al acceso no autorizado.

	CISA advierte sobre 5 fallas de seguridad explotadas activamente	CRÍTICO

Descripción

Se agregaron cinco fallas de seguridad al catálogo de Vulnerabilidades Explotadas Conocidas (KEV), citando evidencia de explotación activa en la naturaleza.

Estado

Esto incluye tres fallas de alta gravedad en el software Veritas Backup Exec Agent (CVE-2021-27876, CVE-2021-27877 y CVE-2021-27878) que podrían conducir a la ejecución de comandos privilegiados en el sistema subyacente. Las fallas se solucionaron en un parche lanzado por Veritas en marzo de 2021.

- CVE-2021-27876 (puntuación CVSS: 8,1): vulnerabilidad de acceso a archivos del agente de Veritas Backup Exec
- CVE-2021-27877 (puntuación CVSS: 8,2): vulnerabilidad de autenticación incorrecta del agente de Veritas Backup Exec
- CVE-2021-27878 (puntuación CVSS: 8,8): vulnerabilidad de ejecución de comandos del agente de Veritas Backup Exec

En un incidente detallado por Mandiant, UNC4466 obtuvo acceso a un servidor de Windows expuesto a Internet, y luego llevó a cabo una serie de acciones que permitieron al atacante implementar la carga útil del ransomware basado en Rust, pero no antes de realizar un reconocimiento, escalar privilegios y deshabilitar Capacidad de monitoreo en tiempo real de Microsoft Defender.

CISA también agregó al catálogo de KEV CVE-2019-1388 (puntaje CVSS: 7.8), una falla de escalada de privilegios que afecta el diálogo de certificado de Microsoft Windows que podría explotarse para ejecutar procesos con permisos elevados en un host ya comprometido.

Remediación / Referencias

Las Agencias del Poder Ejecutivo Federal Civil (FCEB) tienen tiempo hasta el 28 de abril de 2023 para aplicar los parches para proteger sus redes contra amenazas potenciales.

Puedes acceder a toda la información en el siguiente enlace:
https://www.cisa.gov/news-events/alerts/2023/04/07/cisa-adds-five-known-exploited-vulnerabilities-catalog

	**Nueva falla de seguridad del protocolo Wi-Fi que afecta a dispositivos Linux, Android e iOS**	CRÍTICO

Descripción

Se ha revelado una falla de diseño fundamental en el estándar de protocolo Wi-Fi IEEE 802.11, que afecta a una amplia gama de dispositivos que ejecutan Linux, FreeBSD, Android e iOS.

Estado

Se podría abusar de la explotación exitosa de la deficiencia para secuestrar conexiones TCP o interceptar tráfico web y de clientes, dijeron los investigadores Domien Schepers, Aanjhan Ranganathan y Mathy Vanhoef en un artículo publicado esta semana.

El enfoque aprovecha los mecanismos de ahorro de energía en los dispositivos de punto final para engañar a los puntos de acceso para que filtren marcos de datos en texto sin formato, o los cifre usando una clave de cero.

El objetivo es filtrar tramas desde el punto de acceso destinado a una estación de cliente víctima aprovechando el hecho de que la mayoría de las pilas Wi-Fi no eliminan o purgan adecuadamente sus colas de transmisión cuando cambia el contexto de seguridad.

Cisco, en un aviso informativo, describió las vulnerabilidades como un "ataque oportunista y la información obtenida por el atacante tendría un valor mínimo en una red configurada de forma segura".

Sin embargo, la empresa reconoció que los ataques presentados en el estudio pueden tener éxito contra los productos Cisco Wireless Access Point y los productos Cisco Meraki con capacidades inalámbricas.

Remediación / Referencias

Se recomienda implementar la seguridad de la capa de transporte (TLS) para cifrar los datos en tránsito y aplicar mecanismos de cumplimiento de políticas para restringir el acceso a la red.

Por mayor información al respecto se puede acceder a:
https://es.digitaltrends.com/computadoras/wifi-falla-protocolo-permite-robo-trafico-web/

	El nuevo malware MacStealer macOS roba datos y contraseñas del llavero de iCloud	CRÍTICO

Descripción

Un nuevo malware que roba información se ha fijado en el sistema operativo macOS de Apple para desviar información confidencial de los dispositivos comprometidos.

Estado

Anunciado por primera vez en foros de piratería en línea por $100 a principios de mes, todavía es un trabajo en progreso, y los autores de malware planean agregar funciones para capturar datos del navegador Safari de Apple y la aplicación Notes.

En su forma actual, MacStealer está diseñado para extraer datos, contraseñas e información de tarjetas de crédito del llavero de iCloud de navegadores como Google Chrome, Mozilla Firefox y Brave. También cuenta con soporte para recopilar archivos, imágenes, archivos y scripts de Python de Microsoft Office.

Se desconoce el método exacto utilizado para entregar el malware, pero se propaga como un archivo DMG (weed.dmg) que, cuando se ejecuta, abre una solicitud de contraseña falsa para

recolectar las contraseñas con el pretexto de buscar acceso a la aplicación Configuración del sistema.

MacStealer es uno de varios ladrones de información que han surgido en los últimos meses y se suma a una gran cantidad de herramientas similares actualmente en circulación.

Remediación / Referencias

Para mitigar tales amenazas, se recomienda que los usuarios mantengan su sistema operativo y software de seguridad actualizados y eviten descargar archivos o hacer clic en enlaces de fuentes desconocidas.

Puedes acceder a toda la información en el siguiente enlace:
https://www.cisa.gov/news-events/alerts/2023/04/07/cisa-adds-five-known-exploited-vulnerabilities-catalog

JS JavaScript	**Descubren una falla crítica de ejecución remota de código en la biblioteca Sandbox de vm2**	CRÍTICO

Descripción

Los mantenedores del módulo de espacio aislado de JavaScript vm2 han enviado un parche para abordar una falla crítica que podría abusar para romper los límites de seguridad y ejecutar shellcode arbitrario.

Estado

La falla, que afecta a todas las versiones, incluida y anterior a la 3.9.14, fue informada por investigadores de KAIST WSP Lab , con sede en Corea del Sur , el 6 de abril de 2023, lo que llevó a vm2 a publicar una solución con la versión 3.9.15 el viernes.

A la vulnerabilidad se le ha asignado el CVE-2023-29017 identificado y tiene una calificación de 9.8 en el sistema de puntuación CVSS. El problema surge del hecho de que no maneja adecuadamente los errores que ocurren en las funciones asincrónicas.

vm2 es una biblioteca popular que se usa para ejecutar código que no es de confianza en un entorno aislado en Node.js. Tiene casi cuatro millones de descargas semanales y se utiliza en 721 paquetes.

Remediación / Referencias

La divulgación se produce casi seis meses después de que vm2 resolviera otro error crítico (CVE-2022-36067, puntuación CVSS: 10) que podría haber sido un arma para realizar operaciones arbitrarias en la máquina subyacente.

Por mayor información al respecto se puede acceder a:
https://blog.segu-info.com.ar/2023/04/vulnerabilidad-critica-10-en-biblioteca.html

3CX	**Aplicación de escritorio 3CX utilizada en un ataque a la cadena de suministro**	CRÍTICO

Descripción

Se ha descubierto que la aplicación de escritorio 3CX puede verse comprometida y utilizada en ataques a la cadena de suministro.

Estado

La aplicación de escritorio 3CX es un tipo de aplicación de Voz sobre Protocolo de Internet (VoIP) que está disponible para Windows, macOS, Linux y dispositivos móviles. Muchas grandes corporaciones lo usan internamente para hacer llamadas, ver el estado de los colegas, chatear, organizar conferencias web y para el correo de voz. 3CX es un sistema de central telefónica privada (PBX), que es básicamente una red telefónica privada utilizada dentro de una empresa u organización.

El sitio web de 3CX cuenta con 600.000 empresas clientes con 12 millones de usuarios diarios, lo que podría darle una idea del posible impacto que podría tener un ataque a la cadena de suministro.

El ataque descubierto es muy complejo y probablemente ha estado ocurriendo durante meses. Si bien la atribución en estos casos siempre es difícil, algunos dedos apuntan a Corea del Norte. Es probable que los ataques hayan estado en curso desde que una de las muestras compartidas se firmó digitalmente el 3 de marzo de 2023, con un certificado legítimo de 3CX Ltd emitido por DigiCert.

Si bien es casi seguro que los clientes de Windows Electron se vean afectados, hasta el momento no hay evidencia de que otras plataformas lo estén. En los foros de 3CX, se les dice a los usuarios que solo la nueva versión (aplicación de escritorio 3CX) conduce a la infección de malware, porque el teléfono 3CX para Windows (la versión heredada) no se

basa en Electron Framework. Electron es un proyecto de código abierto que permite a los desarrolladores web crear aplicaciones de escritorio.

El ejecutable principal no es malicioso en sí mismo y se puede descargar desde el sitio web de 3CX como parte de un procedimiento de instalación o una actualización. El ejecutable 3CXDesktopApp.exe, sin embargo, descarga una biblioteca de enlaces dinámicos (DLL) maliciosa llamada ffmpeg.dll.

Remediación / Referencias

Después de minimizar inicialmente las alertas en sus foros de usuarios como posibles falsos positivos, 3CX ahora ha publicado que está trabajando en una actualización.

Se aconseja desinstalar la aplicación y luego instalarla, acompañado de un fuerte consejo para instalar el cliente PWA en su lugar.

Por mayor información al respecto se puede acceder a:
https://blog.segu-info.com.ar/2023/04/ataque-la-cadena-de-suministro-de-voip.html

	Apple lanza actualizaciones para abordar fallas de día cero en iOS, iPadOS, macOS y Safari	PREVENCIÓN

Descripción

Apple lanzó el viernes actualizaciones de seguridad para iOS, iPadOS , macOS y el navegador web Safari para abordar un par de fallas de día cero que se están explotando en la naturaleza.

Estado

Las dos vulnerabilidades son las siguientes:

- CVE-2023-28205: un uso después de un problema gratuito en WebKit que podría conducir a la ejecución de código arbitrario al procesar contenido web especialmente diseñado.
- CVE-2023-28206: un problema de escritura fuera de los límites en IOSurfaceAccelerator que podría permitir que una aplicación ejecute código arbitrario con privilegios de kernel.

Apple dijo que abordó CVE-2023-28205 con una gestión de memoria mejorada y el segundo con una mejor validación de entrada, y agregó que sabe que los errores "pueden haber sido explotados activamente".

Remediación / Referencias

Las actualizaciones están disponibles en la versión iOS 16.4.1, iPadOS 16.4.1, macOS Ventura 13.3.1 y Safari 16.4.1.

Por mayor información al respecto se puede acceder a:
https://support.apple.com/en-il/HT213720

Microsoft	Microsoft corrige una nueva vulnerabilidad de Azure AD	PREVENCIÓN

Descripción

Microsoft solucionó un problema de configuración incorrecta que afectaba el servicio de gestión de acceso e identidad de Azure Active Directory (AAD) que exponía varias aplicaciones de "alto impacto" al acceso no autorizado.

Estado

Los problemas se informaron a Microsoft en enero y febrero de 2022, luego de lo cual aplicó correcciones y otorgó a Wiz una recompensa por errores de $40,000.

El quid de la vulnerabilidad se deriva de lo que se denomina "confusión de responsabilidad compartida", en la que una aplicación de Azure puede configurarse incorrectamente para permitir a los usuarios de cualquier inquilino de Microsoft, lo que lleva a un caso potencial de acceso no deseado.

Curiosamente, se descubrió que varias aplicaciones internas de Microsoft mostraban este comportamiento, lo que permitía a terceros obtener lectura y escritura en las aplicaciones afectadas.

Esto incluye la aplicación Bing Trivia, que la empresa de ciberseguridad explotó para alterar los resultados de búsqueda en Bing e incluso manipular el contenido de la página de inicio como parte de una cadena de ataque denominada BingBang.

Otras aplicaciones propiedad de Microsoft que se encontraron susceptibles al problema de configuración incorrecta incluyen Mag News, Central Notification Service (CNS), Contact Center, PoliCheck, Power Automate Blog y COSMOS.

Remediación / Referencias

La investigación también sigue al lanzamiento de parches para remediar Super FabriXss (CVE-2023-23383, puntaje CVSS: 8.2), una vulnerabilidad XSS reflejada en Azure Service Fabric Explorer (SFX) que podría conducir a la ejecución remota de código no autenticado.

Por mayor información al respecto se puede acceder a:
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-36949

Conclusiones

Hemos visto como los boletines tempranos de ciberseguridad como este ayudan a las organizaciones a tomar medidas a tiempo efectivas.
Reducir las oportunidades de posibles ataques en el corto plazo es una tarea fundamental, ya que los atacantes no pierden un segundo en reconocer y detectar infraestructuras vulnerables para atacarlas lo más rápido posible y tomar control de las mismas.

Las organizaciones modernas requieren de información precisa y rápida de las amenazas a las que se enfrentan en este mundo globalizado. Es imprescindible contar con noticias de seguridad de todos nuestros productos de software y hardware que utilicemos, ya que una vulnerabilidad crítica en uno de ellos podría afectar a toda la organización con pérdidas totales.

Tal es el caso de 3CX en dónde por una intrusión no autorizada, se modificó el código del programa de telefonía principal de la organización, y este programa se descargó por todos los clientes de 3CX. Lo que hizo saltar todas las alarmas, ya que la medida de contención inicialmente es la de desinstalar el producto en cada sistema que lo tuviera, y esto es porque el software se actualiza automáticamente, y esa actualización contiene el malware.
Riesgos como este de 3CX se están viendo y se verán más a menudo en todas las tecnologías que usemos. Es por eso tan importante saber que hacer en cada caso lo antes posible, ya que la gestión de vulnerabilidades es una carrera contra el tiempo; el tiempo en que expongamos una posible brecha que pueda ser comprometida fácilmente debería ser siempre el menos posible.

Para todo esto y mucho más, en Datasec aportamos valor a las organizaciones en reducir estas brechas al máximo, dejando poca o ninguna posibilidad u oportunidad a adversarios.