Boletín de Ciberseguridad

Fecha de Publicación
17/01/2022 - N.º 25

Mes de Enero
03/01/2022 - 17/01/2022

Datasec

Índice

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 segunda quincena del mes de enero se destacan 8 noticias de relevancia: 4 sobre vulnerabilidades tecnológicas y 4 de prevención.

Aquellas noticias a tener especial recaudo son las siguientes:

Microsoft reporta error RCE crítico y 6 días cero

Microsoft ha abordado un total de 97 vulnerabilidades de seguridad en su actualización de parches en enero de 2022, nueve de ellas calificadas como críticas, incluidas seis que se enumeran como “día cero" conocidas públicamente.

Vulnerabilidad en Cisco que permite escalar privilegios

Una vulnerabilidad en la interfaz de administración basada en web de Cisco Unified Contact Center Management Portal (Unified CCMP) y Cisco Unified Contact Center Domain Manager (Unified CCDM) podría permitir que un atacante remoto eleve sus privilegios a Administrador.

Nuevo malware de espionaje SysJoker dirigido a usuarios de Windows, macOS y Linux

Nueva puerta trasera multiplataforma llamada "SysJoker" dirigida a máquinas que ejecutan sistemas operativos Windows, Linux y macOS como parte de una campaña de espionaje en curso

Microsoft	**Microsoft reporta error RCE crítico y 6 Zero Days**	CRÍTICO

Descripción

Microsoft ha abordado un total de 97 vulnerabilidades de seguridad en su actualización de parches en enero de 2022, nueve de ellas calificadas como críticas, incluidas seis que se enumeran como "día cero'' conocidas públicamente.

Estado

Las correcciones incluyen a Microsoft Windows y componentes de Windows, Microsoft Edge (basado en cromo), Exchange Server, Microsoft Office y componentes de Office, SharePoint Server, .NET Framework, Microsoft Dynamics, software de código abierto, Windows Hyper-V, Windows Defender y Protocolo de escritorio remoto (RDP) de Windows.

De los errores críticos, se destaca un problema de ejecución remota de código (RCE) en la pila del protocolo HTTP, dado que es compatible con gusanos, es decir, un exploit podría auto propagarse a través de una red sin interacción del usuario. Tiene la calificación de gravedad de vulnerabilidad CVSS más grave de toda la actualización, con un 9,8 en una escala de 10 puntos.

El error se puede explotar enviando paquetes especialmente diseñados a un sistema que utiliza la pila de protocolos HTTP (http.sys) para procesar paquetes. El bug tiene como objetivo la función de

compatibilidad con el tráiler de HTTP, que permite que un remitente incluya campos adicionales en un mensaje para proporcionar metadatos, proporcionando un mensaje que puede conducir a la ejecución remota de código sin la necesidad de ninguna interacción por parte del usuario.

Remediación / Referencias

Aunque Microsoft ha proporcionado un parche oficial, este error es otro recordatorio de que las características del software brindan oportunidades para que los atacantes hagan un mal uso de las funcionalidades para actos maliciosos.
Se recomienda un parcheo inmediato, haciendo uso de la siguiente guía de Microsoft: https://msrc.microsoft.com/update-guide/

Por mayor información acceder a:
https://threatpost.com/microsoft-wormable-critical-rce-bug-zero-day/177564/

	**Error de RDP de Windows expone a los usuarios al robo de datos**	IMPORTANTE

Descripción

La mayoría de las versiones de Windows corren el riesgo de que atacantes remotos y sin privilegios abusen de RDP desde adentro para secuestrar tarjetas inteligentes y obtener acceso no autorizado al sistema de archivos.

Estado

El *Remote Desktop Protocol* (RDP) tiene un error de seguridad que podría permitir que cualquier usuario estándar y sin privilegios acceda a las máquinas de otros usuarios conectados. Si se explota, podría generar problemas de privacidad de datos, movimiento lateral y escalada de privilegios, advirtieron los investigadores.

Los atacantes internos podrían, por ejemplo, ver y modificar los datos del portapapeles de otras personas o hacerse pasar por otros usuarios registrados utilizando tarjetas inteligentes.

Sin embargo, Microsoft afirmó que una explotación de la vulnerabilidad sería de baja complejidad, lo que lleva a una calificación de criticidad de CVSS de 7.7 sobre 10, lo que lo hace "importante" en gravedad.

Remediación / Referencias

Recomiendan fuertemente aplicar el parche lanzado por Microsoft, dado que casi todas las versiones de Windows están afectadas. Los expertos también sugieren que los desarrolladores de aplicaciones que usan canales virtuales personalizados deberían verificar si son vulnerables y realizar su propia evaluación de seguridad.

Por mayor información al respecto acceder a:
https://msrc.microsoft.com/update-guide/
https://threatpost.com/windows-bug-rdp-exploit-unprivileged-users/177599/

vmware	VMware corrige un error que afecta a los productos ESXi, Workstation y Fusion	IMPORTANTE

Descripción

VMWare ha enviado actualizaciones a los productos Workstation, Fusion y ESXi para abordar una vulnerabilidad de seguridad que podría ser armada por un actor de amenazas para tomar el control de los sistemas afectados.

Estado

El problema se relaciona con una vulnerabilidad de desbordamiento de memoria, y tiene un puntaje de riesgo evaluado en CVSS: 7.7, que de ser explotado con éxito, da como resultado la ejecución de código arbitrario.

Un actor malintencionado con acceso a una máquina virtual con emulación de dispositivo de CD-ROM puede explotar esta vulnerabilidad junto con otros problemas para ejecutar código en el hipervisor desde una máquina virtual, la explotación exitosa requiere que una imagen de CD se adjunte a la máquina virtual.

Remediación / Referencias

El error afecta a las versiones 6.5, 6.7 y 7.0 de ESXi; versiones 16.x de estaciones de trabajo; y versiones 12.x de Fusion, con la compañía aún por lanzar un parche para ESXi 7.0.
Mientras tanto, la compañía recomienda a los usuarios que deshabiliten todos los dispositivos de CD-ROM/DVD en todas las máquinas virtuales en ejecución para evitar cualquier posible explotación. Y parchear las versiones que si se encuentran controladas en: https://customerconnect.vmware.com/

Para saber más:
https://thehackernews.com/2022/01/vmware-patches-important-bug-affecting.html

cisco	**Vulnerabilidad en Cisco permite escalar privilegios sin autorización**	IMPORTANTE

Descripción

Una vulnerabilidad en la interfaz de administración basada en web de Cisco Unified Contact Center Management Portal (Unified CCMP) y Cisco Unified Contact Center Domain Manager (Unified CCDM) podría permitir que un atacante remoto eleve sus privilegios a Administrador.

Afectados

Esta vulnerabilidad afecta a Cisco Unified CCMP y Cisco Unified CCDM si se ejecutan con la configuración predeterminada.

Estado

Esta vulnerabilidad se debe a la falta de validación del lado del servidor de los permisos de usuario.

Un atacante podría aprovechar esta vulnerabilidad enviando una solicitud HTTP manipulada a un sistema vulnerable. Una explotación exitosa podría permitir al atacante crear cuentas de administrador. Con estas cuentas, podría acceder y modificar la telefonía y los recursos de usuario en todas las plataformas unificadas que están asociadas al Cisco Unified CCMP vulnerable. Para explotar con éxito esta vulnerabilidad, un atacante necesitaría credenciales de usuario avanzadas válidas.

Remediación / Referencias

Cisco ha lanzado actualizaciones de software gratuitas que abordan la vulnerabilidad descrita.
Los clientes con contratos de servicio que les dan derecho a actualizaciones periódicas de software deben obtener soluciones de seguridad a través de sus canales de actualización habituales, sin la posibilidad de soluciones alternativas que aborden la misma.

Puedes acceder a toda la información en el siguiente enlace:
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ccmp-priv-esc-JzhTFLm4
https://www.cisco.com/c/en/us/support/index.html

	Malware de espionaje SysJoker dirigido a usuarios de Windows, macOS y Linux	PREVENCIÓN

Descripción

Nueva puerta trasera multiplataforma llamada "SysJoker" dirigida a máquinas que ejecutan sistemas operativos Windows, Linux y macOS como parte de una campaña de espionaje en curso.

Estado

Los investigadores informan que *SysJoker* se hace pasar por una actualización del sistema y genera su servidor de comando y control al decodificar una cadena recuperada de un archivo de texto alojado en Google Drive.

SysJoker, un malware basado en C++, se entrega a través de un archivo cuentagotas desde un servidor remoto que, al ejecutarse, está diseñado para recopilar información sobre el host comprometido, como la dirección MAC, el nombre de usuario, el número de serie del medio físico y la dirección IP, todo de los cuales se codifican y se transmiten de vuelta al servidor.

Además, las conexiones con el servidor controlado por el atacante se establecen extrayendo la URL del dominio de un enlace de Google Drive codificado que aloja un archivo de texto ("dominio.txt"), lo que permite que el servidor transmita instrucciones a la máquina que permiten el malware para ejecutar comandos y ejecutables arbitrarios, después de lo cual se transmiten los resultados.

Especialistas afirman que el hecho de que el código se haya escrito desde cero, no se haya visto antes en otros ataques y no hayan evidencias de una segunda etapa o comando enviado por el atacante, sugiere que el ataque es específico, lo que generalmente encaja para un actor avanzado.

Por mayor información al respecto se puede acceder a:
https://thehackernews.com/2022/01/new-sysjoker-espionage-malware.html

iPhone	**Truco permite que malware falsifique el apagado del iPhone para espiar a usuarios**	PREVENCIÓN

Descripción

Los investigadores han revelado una técnica mediante la cual el malware en iOS puede persistir en un dispositivo infectado al simular su proceso de apagado, lo que hace imposible determinar físicamente si un iPhone está apagado o no.

Estado

Fue descubierto un malware, denominado "NoReboot", que cuenta con un comportamiento de falsificación y camuflaje, en dónde simula una operación de reinicio de iOS, engañando al usuario haciéndole creer que el teléfono se apagó cuando, en realidad, todavía está prendido y posiblemente grabando con las cámaras, entre otras funciones.

NoReboot funciona interfiriendo con las rutinas utilizadas en iOS para apagar y reiniciar el dispositivo, lo que evita que sucedan en primer lugar y permite que un troyano logre persistencia sin persistencia ya que el dispositivo nunca se apaga.

Esto se logra inyectando un código especialmente diseñado en iOS: *InCallService*, *SpringBoard* y *Backboardd*, para simular un apagado al deshabilitar todas las señales audiovisuales asociadas con un dispositivo encendido, incluida la pantalla, los sonidos, la vibración, el indicador de la cámara y la retroalimentación táctil.

Buscan dar la impresión de que el dispositivo se apagó sin apagarlo realmente al secuestrar el evento que se activa cuando el usuario presiona y mantiene presionados simultáneamente el botón lateral y uno de los botones de volumen, y arrastra el "deslizante para apagar".El teléfono sigue siendo completamente funcional y es capaz de mantener una conexión a Internet activa engañando al usuario haciéndole creer que el teléfono está apagado, ya sea porque la víctima lo apagó o porque los actores maliciosos usaron 'batería baja' como excusa.

Remediación / Referencias

Aunque hasta la fecha no se ha detectado ni documentado públicamente ningún malware utilizando un método similar a *NoReboot*, los hallazgos destacan que incluso el proceso de reinicio de iOS no es inmune a ser secuestrado una vez que un adversario ha obtenido acceso a un dispositivo de destino, algo que está al alcance de grupos de ciberdelincuentes.

Para saber más:
https://support.apple.com/en-us/HT201222
https://thehackernews.com/2022/01/new-trick-could-let-malware-fake-iphone.html

	**Actualización de Chrome parchea nuevas vulnerabilidades del navegador**	PREVENCIÓN

Descripción

Google lanzó la primera ronda de actualizaciones de su navegador web Chrome para 2022 para solucionar 37 problemas de seguridad, uno de los cuales tiene una gravedad crítica y podría explotarse para pasar código arbitrario y obtener control sobre el sistema de una víctima.

Estado

La falla crítica se relaciona con un error de uso posterior a la liberación en el componente de almacenamiento, que podría tener efectos devastadores que van desde la corrupción de datos válidos hasta la ejecución de código malicioso en una máquina comprometida.

Remediación / Referencias

Se recomienda a los usuarios de Chrome que actualicen a la última versión 97.0.4692.71 para Windows, Mac y Linux dirigiéndose a Configuración > Ayuda > "Acerca de Google Chrome" para mitigar cualquier riesgo potencial de explotación activa.

Por más información:
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-0096
https://thehackernews.com/2022/01/google-releases-new-chrome-update-to.html

Actualizaciones de Apple parchean vulnerabilidad DoS de HomeKit

PREVENCIÓN

Descripción

Apple lanzó el miércoles actualizaciones de software para iOS y iPadOS para remediar un problema persistente de denegación de servicio (DdoS) que afecta el marco del hogar inteligente HomeKit, el cual podría ser explotado para lanzar ataques de tipo ransomware dirigidos a los dispositivos.

Estado

El fabricante de iPhone, en sus notas de lanzamiento para iOS y iPad OS 15.2.1, lo calificó como un "problema de agotamiento de recursos" que podría desencadenarse al procesar un nombre de accesorio de HomeKit creado con fines malintencionados, y agregó que solucionó el error con una validación mejorada.

La llamada vulnerabilidad "doorLock", afecta al HomeKit, la API de software para conectar dispositivos domésticos inteligentes a aplicaciones iOS.

Si se explota con éxito, los iPhones y iPads pueden caer en una espiral de choque simplemente cambiando el nombre de un dispositivo HomeKit a una cadena de más de 500,000 caracteres y engañando al objetivo para que acepte una invitación de Home maliciosa.

Peor aún, dado que los nombres de los dispositivos de HomeKit están respaldados en iCloud, volver a iniciar sesión en la cuenta de iCloud afectada vinculada al dispositivo HomeKit puede volver a activar la condición DoS y hacer que los dispositivos entren en un ciclo interminable de bloqueo y reinicio que solo puede finalizar restaurándolos a su configuración de fábrica.

Aunque la empresa intentó mitigar el problema introduciendo un límite en la longitud del nombre que puede establecer una aplicación o el usuario, se descubrió que no hizo nada para evitar que un atacante ejecute una versión anterior que permite nombres de dispositivos excesivamente largos y luego hacer que la víctima acepte una invitación deshonesta a través de un correo electrónico de phishing.

Remediación / Referencias

Se deberá parchear los dispositivos a la última actualización lanzada por Apple, a través de https://support.apple.com/en-us/HT213043

Por mayor información:
https://www.theverge.com/2022/1/12/22880493/apple-15-2-1-patch-ios-homekit-denial-of-service-vulnerability-fix
https://thehackernews.com/2022/01/apple-releases-iphone-and-ipad-updates.html

Conclusiones

Esta nueva quincena de noticias vino cargada con varias referentes a la gestión y actualización de vulnerabilidades de software conocido y popular. Para trabajar estos procesos dentro de nuestras organizaciones, son claves algunos elementos y herramientas de gestión operativa, para poder así balancear la economía y los riesgos.

Muchos expertos recomendamos contar con inventario de software y versiones utilizadas en cada uno de nuestros activos más importantes, lo que permitirá evaluar cuándo, dónde y cómo se realizarán actualizaciones de seguridad.
Otra clave son las herramientas de gestión y automatización de estos procesos, ya que los mismos son constantes; mes a mes existen actualizaciones críticas a implementar para así evitar riesgos mayores en las plataformas de sistemas operativos y aplicaciones principales de la operativa. Esto sucede tanto a nivel de los servidores y servicios que provee la organización, así como en los equipos finales de nuestros empleados y proveedores; es decir que estos también contarán con actualizaciones en sus móviles, PCs, etc.

Muchas organizaciones tienen equipos especializados para evaluar e implementar parches y actualizaciones de seguridad, ya que esta tarea suele implicar tiempos ajustados, pruebas de funcionamiento, ventanas de mantenimiento, comunicaciones a clientes y demás interesados. Cuanto más aceitado y fluido sea este proceso manejado en nuestras organizaciones, acelerará los procesos de cambios tecnológicos, aumentará el cumplimiento y la reducción efectiva de riesgos tecnológicos.

Desde Datasec seguimos dando seguridad a organizaciones latinoamericanas, elevando así la postura de ciberseguridad en varios ámbitos.

¡Hasta la próxima quincena!