Boletín de Ciberseguridad

Fecha de Publicación
09/05/2022- N.º 33

Mes de Mayo
25/04/2022 -09/05/2022

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 mayo se destacan 7 noticias de relevancia: 2 sobre vulnerabilidades tecnológicas y 5 de prevención.

Aquellas noticias a tener especial recaudo son las siguientes:

Se revelan vulnerabilidades de hace años en Avast y AVG Antivirus

Se han descubierto dos vulnerabilidades de seguridad de alta gravedad, que pasaron desapercibidas durante varios años, en un controlador legítimo que forma parte de las soluciones antivirus de Avast y AVG.

Millones de aplicaciones Java siguen siendo vulnerables a Log4Shell

Cuatro meses después del descubrimiento de la falla crítica Log4Shell, millones de aplicaciones Java siguen siendo vulnerables al compromiso.

Los sistemas F5 BIG-IP son vulnerables a control remoto no autorizado

El proveedor de líder en control de tráfico, y seguridad de aplicaciones F5, ha emitido parches para su plataforma BIG-IP, para abordar un error crítico que podría utilizarse para comprometer y controlar de forma remota los sistemas vulnerables.

avast	**Se revelan vulnerabilidades de hace años en Avast y AVG Antivirus**	CRÍTICO

Descripción

Se han descubierto dos vulnerabilidades de seguridad de alta gravedad, que pasaron desapercibidas durante varios años, en un controlador legítimo que forma parte de las soluciones antivirus de Avast y AVG.

Estado

Rastreadas como CVE-2022-26522 y CVE-2022-26523, las fallas residen en un controlador de kernel anti-rootkit legítimo llamado aswArPot.sys y se dice que se introdujeron en la versión 12.1 de Avast, que se lanzó en junio de 2016.

Específicamente, las deficiencias tienen su origen en un controlador de conexión de socket en el controlador del kernel que podría conducir a una escalada de privilegios al ejecutar código en el kernel de un usuario que no sea administrador, lo que podría causar que el sistema operativo se bloquee y muestre una pantalla azul de muerte (BSoD) error.
De manera preocupante, las fallas también podrían explotarse como parte de un ataque de navegador de segunda etapa o para realizar un escape de sandbox, lo que tendría consecuencias de largo alcance.

Remediación / Referencias

Si bien estas vulnerabilidades no han sido explotadas en la realidad corporativa, hasta ahora, son decenas de millones de usuarios afectados.
Es posible que los atacantes busquen a aquellos que no toman las medidas adecuadas.

Por mayor información acceder a:
https://therecord.media/avast-avg-release-security-updates-for-decade-old-vulnerability/

Microsoft	**Microsoft descubre falla de escalada de privilegios en el sistema operativo Linux**	CRÍTICO

Descripción

Microsoft reveló el martes pasado un conjunto de dos vulnerabilidades, que permiten la escalada de privilegios en el sistema operativo Linux, esto podrían permitir a los actores de amenazas llevar a cabo una serie de actividades nefastas.

Estado

Las vulnerabilidades tienen sus raíces en un componente de systemd llamado networkd-dispatche, un programa tipo daemon que ejecuta el servicio de administrador de red, que está diseñado para enviar cambios de estado de la red.

Específicamente, se relacionan con una combinación de fallas del tipo atravesamiento de directorios (CVE-2022-29799), así como otras fallas sobre la verificación del tiempo de uso (CVE-2022-29800), lo que lleva a un escenario en el que un adversario que tiene el control de un servicio D-Bus no autorizado puede plantar y ejecutar puertas traseras maliciosas en los puntos finales comprometidos.

Remediación / Referencias

Se recomienda encarecidamente a los usuarios de networkd-dispatcher que actualicen sus instancias a la última versión para mitigar el potencial que surge de la explotación de las fallas.

Por mayor información acceder a:
https://www.microsoft.com/security/blog/2022/04/26/microsoft-finds-new-elevation-of-privilege-linux-vulnerability-nimbuspwn/

Java	**Millones de aplicaciones Java siguen siendo vulnerables a Log4Shell**	PREVENCIÓN

Descripción

Cuatro meses después del descubrimiento de la falla crítica Log4Shell, millones de aplicaciones Java siguen siendo vulnerables al compromiso.

Estado

Rezilion analizó el estado actual de ataques probables para la vulnerabilidad en el conocido software libre Apache Struts, que amenazó con dividir Internet cuando se descubrió en diciembre. La falla en la omnipresente biblioteca utilizada para registros de Java; Apache Log, se puede explotar rápidamente y puede permitir la ejecución remota de código (RCE) no autenticado y el control total del servidor, en ciertas versiones vulnerables.

Bastantes aplicaciones continúan utilizandoLog4J versión 1.x y probablemente no estén parcheadas porque la vulnerabilidad original de Log4Shell, rastreada como CVE-201-44228, no se aplica a esta versión.
Sin embargo, esto es un malentendido ya que ese modelo ha estado "en un punto de finalización de la vida útil desde agosto de 2015" (lo que significa que no recibe ninguna actualización de seguridad) y contiene muchas otras vulnerabilidades, incluidas las vulnerabilidades RCE.

Remediación / Referencias

Actualmente, todavía existen docenas de intentos de explotación diarios registrados de Log4Shell.
Impulsar e implementar las actualizaciones de esta librería hacia versiones seguras hoy en día.

Para saber más invitamos a visitar el siguiente sitio:
https://cso.computerworld.es/cibercrimen/una-vulnerabilidad-afecta-a-millones-de-aplicaciones-basadas-en-java
https://devops.com/report-finds-most-log4shell-vulnerabilities-unpatched/

	**Propagación del malware 'Raspberry Robin' a través de unidades externas**	PREVENCIÓN

Descripción

Investigadores de ciberseguridad han descubierto un nuevo malware de Windows con capacidades similares a las de un gusano y se propaga por medio de dispositivos USB extraíbles.

Estado

Al atribuir el malware a un grupo llamado "Raspberry Robin", los investigadores de Red Canary señalaron que el gusano "aprovecha Windows Installer para llegar a los dominios asociados con QNAP y descargar una DLL maliciosa".

Se dice que los primeros signos de la actividad se remontan a septiembre de 2021, con infecciones observadas en organizaciones vinculadas a los sectores tecnológico y manufacturero.

Las cadenas de ataque relacionadas con Raspberry Robin comienzan con la conexión de una unidad USB infectada a una máquina con Windows. Presente dentro del dispositivo está la carga útil del gusano, que aparece como un archivo de acceso directo .LNK a una carpeta legítima.

Luego, el gusano se encarga de generar un nuevo proceso usando cmd.exe para leer y ejecutar un archivo malicioso almacenado en la unidad externa.

A esto le sigue el lanzamiento de explorer.exe y msiexec.exe, el último de los cuales se usa para la comunicación de red externa a un dominio no autorizado para fines de comando y control (C2) y para descargar e instalar un archivo de biblioteca DLL.

La DLL maliciosa se carga y ejecuta posteriormente mediante una cadena de utilidades legítimas de Windows, como fodhelper.exe, rundll32.exe a rundll32.exe y odbcconf.exe, omitiendo efectivamente el Control de cuentas de usuario (UAC).

Remediación / Referencias

A través de los IOC publicados es posible detectar y actuar en contra de esta amenaza, a través de software XDR o SIEM especialmente configurados. También software antimalware con los IOC actualizados sobre esta amenaza podrán responder a la misma.

Para saber más invitamos a visitar el siguiente sitio:
https://zonaactual.es/el-gusano-raspberry-robin-se-propaga-a-traves-de-windows-installer/
https://redcanary.com/blog/raspberry-robin/

	**Actualización de Android para parchear vulnerabilidad**	PREVENCIÓN

Descripción

Google ha lanzado parches de seguridad mensuales para Android con correcciones para 37 fallas en diferentes componentes, una de las cuales es una corrección para una vulnerabilidad del kernel de Linux explotada activamente que salió a la luz a principios de este año.

Estado

Registrada como CVE-2021-22600 (puntuación CVSS: 7,8), la vulnerabilidad está clasificada como "Alta" por su gravedad y podría ser explotada por un usuario local para aumentar los privilegios o denegar los servicios.

El problema se relaciona con una vulnerabilidad de doble liberación que reside en la implementación del protocolo de red Packet en el kernel de Linux que podría causar daños en la memoria, lo que podría provocar una denegación de servicio o la ejecución de código arbitrario.

Los parches fueron lanzados por diferentes distribuciones de Linux, incluidas Debian, Red Hat, SUSE y Ubuntu en enero de 2022.

Remediación / Referencias

También se corrigieron como parte de los parches de este mes otros tres errores en el núcleo, así como 18 fallas de alta gravedad y una de gravedad crítica en los componentes de MediaTek y Qualcomm.

Para saber más invitamos a visitar el siguiente sitio:
https://source.android.com/security/bulletin/2022-05-01

Cisco publica parches para 3 nuevas fallas que afectan el software NFVIS empresarial

PREVENCIÓN

Descripción

Cisco Systems envió el miércoles parches de seguridad para contener tres fallas que afectan su software de infraestructura Enterprise NFV (NFVIS) que podría permitir que un atacante aproveche por completo este agujero, y tome el control de los sistemas.

Estado

Rastreadas como CVE-2022-20777, CVE-2022-20779 y CVE-2022-20780, las vulnerabilidades "podrían permitir que un atacante escape de la máquina virtual (VM) a la máquina host, inyectar comandos que se ejecutan en la raíz o filtrar datos del sistema del host a la VM", dijo la compañía.

Cyrille Chatras, Pierre Denouel y Loïc Restoux de Orange Group son acreditados por descubrir y reportar los problemas. Se han publicado actualizaciones en la versión 4.7.1.

La compañía de equipos de red dijo que las fallas afectan a Cisco Enterprise NFVIS en la configuración predeterminada. Los detalles de los tres errores son los siguientes:

- CVE-2022-20777 (puntuación CVSS: 9,9): un problema con restricciones de invitado insuficientes que permite que un atacante remoto autenticado escape de la máquina virtual invitada para obtener acceso no autorizado a nivel raíz en el host NFVIS.

- CVE-2022-20779 (puntaje CVSS: 8.8): una falla de validación de entrada incorrecta que permite que un atacante remoto no autenticado inyecte comandos que se ejecutan en el nivel raíz en el host NFVIS durante el proceso de registro de imágenes.

- CVE-2022-20780 (puntuación CVSS: 7,4): una vulnerabilidad en la función de importación de Cisco Enterprise NFVIS que podría permitir que un atacante remoto no autenticado acceda a la información del sistema desde el host en cualquier máquina virtual configurada.

Remediación / Referencias

Se aconseja a los usuarios de los dispositivos Catalyst 2960X/2960XR a actualizar su software a IOS versión 15.2(7)E4 o posterior para habilitar nuevas funciones de seguridad.

Para saber más invitamos a visitar el siguiente sitio:
https://www.cert.gov.py/noticias/multiples-vulnerabilidades-en-productos-cisco-3

	Sistemas F5 BIG-IP vulnerables control remoto	PREVENCIÓN

Descripción

El proveedor de control de tráfico, y seguridad de aplicaciones F5 ha emitido parches para su plataforma BIG-IP, para abordar un error crítico que permitiría el control remoto de los sistemas vulnerables.

Estado

La falla radica en la interfaz de transferencia de estado representacional (REST) para la función iControl, que se utiliza para interactuar entre usuarios o scripts y dispositivos F5.

Los usuarios no autenticados que pueden acceder al puerto de administración de los sistemas BIG-IP de F5 o a las "direcciones IP propias" podrían omitir la autenticación REST de iControl.

Una dirección IP propia es una dirección IP en el sistema BIG-IP que los clientes asocian con una VLAN para acceder a los hosts en esa VLAN.

La omisión de autenticación permite a los atacantes ejecutar comandos arbitrarios en elsistema, crear o eliminar archivos y deshabilitar servicios en sistemas BIG-IP vulnerables.

Las ramas de software 13.x - 16.x tienen versiones vulnerables con el error presente, que tiene una calificación de 9.8 sobre 10 en el Sistema de puntuación de vulnerabilidades comunes (CVSS) versión 3.90.

Productos afectados:

- BIG-IP versions 16.1.0 a16.1.2
- BIG-IP versions 15.1.0 a15.1.5
- BIG-IP versions 14.1.0 a14.1.4
- BIG-IP versions 13.1.0 a13.1.4
- BIG-IP versions 12.1.0 a12.1.6
- BIG-IP versions 11.6.1 a11.6.5

Remediación / Referencias

Se aconsejó a los usuarios aplicar las actualizaciones necesarias para F5 BIG-IP o soluciones alternativas de control de tráfico.

Para saber más invitamos a visitar el siguiente sitio:
https://www.csirt.gob.cl/noticias/alerta-de-seguridad-cibernetica-big-ip/

Conclusión

Nueva quincena, nuevo boletín de ciberseguridad.
En esta oportunidad destacamos la importancia para los equipos de seguridad de las organizaciones, el contar con listado de componentes y versiones de software, de esta manera es que podrán priorizar y agendar ventanas de mantenimiento para aplicar los parches de seguridad apropiados y apropiables para la misma.

Más allá de procesos de actualización de software, y aplicación de parches, vemos cada vez más noticias, en que ya estos procesos no solo son imprescindibles para contar con una postura de ciberseguridad aceptable, sino que se suman a estos procesos los referidos al monitoreo de comportamientos y eventos especiales, que muchos pueden parecer legítimos, pero que su finalidad es con intenciones maliciosas, hablamos de extracción y filtración de información, operaciones fraudulentas que utilicen tecnologías de la información, entre otras.
Por eso el monitoreo de casos de usos para situaciones específicas, está cada vez más de moda en el ámbito de la defensa proactiva de la información. A través de software con cierta inteligencia y operadores que tomen acciones, es que la postura de ciberseguridad de varias organizaciones comienza a ciclar de una forma efectiva.

Es muy importante que la dirección y ejecutivos de las organizaciones protejan sus activos por sobre los límites de los estándares, los vectores de información son muy amplios como para dejar expuestas puertas,

Desde Datasec apoyamos todos los procesos de aseguramiento de la información. Saludamos atentamente a nuestros lectores, y hasta la próxima quincena de noticias de nuestro ámbito.