Boletín de Ciberseguridad

Fecha de Publicación
25/04/2022- N.º 32

Mes de Abril
11/04/2022 -25/04/2022

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 marzo se destacan 6 noticias de relevancia: 4 sobre vulnerabilidades tecnológicas, y 2 de prevención.

Aquellas noticias a tener especial recaudo son las siguientes:

Millones de portátiles Lenovo afectadas por vulnerabilidades del firmware UEFI

Se han descubierto tres vulnerabilidades de seguridad de interfaz de firmware extensible unificada de alto impacto que afectan a varios modelos de portátiles de consumo de Lenovo, lo que permite a los actores maliciosos implementar y ejecutar implantes de firmware en los dispositivos afectados.

Error en Java hace que las firmas digitales no tengan valor

Debido a un error en la implementación de firmas digitales, muchos entornos Java aceptan firmas digitales falsificadas.

Error crítico en el software del controlador de LAN inalámbrica de Cisco

Cisco ha lanzado parches para contener una vulnerabilidad de seguridad crítica que afecta al controlador de LAN inalámbrica (WLC) que podría ser abusada por un atacante remoto no autenticado para tomar el control de un sistema afectado.

	Piratas informáticos explotan vulnerabilidad en Windows Print Spooler	CRÍTICO

Descripción

Una falla de seguridad en el administrador de trabajos de impresión de Windows que fue reparada por Microsoft en febrero, está siendo explotada activamente en la naturaleza.

Estado

Registrada como CVE-2022-22718, la vulnerabilidad de seguridad es una de las cuatro fallas de escalada de privilegios en Print Spooler que Microsoft resolvió como parte de sus actualizaciones del martes de parches el 8 de febrero de 2022.

Se desconocen los detalles sobre los ataques y la identidad de los actores de amenazas que pueden estar explotando el defecto de Print Spooler, en parte en un intento de evitar una mayor explotación por parte de los equipos de piratería. Microsoft, por su parte, le asignó una etiqueta de "explotación más probable" cuando se implementaron las correcciones hace dos meses.

También se agregaron al catálogo otras dos fallas de seguridad basadas en "evidencia de explotación activa":

- CVE-2018-6882 (puntaje CVSS: 6.1): vulnerabilidad de secuencias de comandos entre sitios (XSS) de Zimbra Collaboration Suite (ZCS)
- CVE-2019-3568 (puntuación CVSS: 9,8): vulnerabilidad de desbordamiento de búfer de pila VOIP de WhatsApp

Remediación / Referencias

Debido a los ataques que utilizan las vulnerabilidades como armas, se recomienda a las organizaciones que reduzcan su exposición.

Por mayor información acceder a:
https://cultura-informatica.com/windows/impresion-de-windows/

Lenovo	Millones de portátiles Lenovo afectadas por vulnerabilidades del firmware UEFI	CRÍTICO

Descripción

Se han descubierto tres vulnerabilidades de seguridad de interfaz de firmware extensible unificada de alto impacto que afectan a varios modelos de portátiles de consumo de Lenovo, lo que permite a los actores maliciosos implementar y ejecutar implantes de firmware en los dispositivos afectados.

Estado

Registrados como CVE-2021-3970, CVE-2021-3971 y CVE-2021-3972, los dos últimos afectan los controladores de firmware originalmente destinados a usarse solo durante el proceso de fabricación de las computadoras portátiles de consumo de Lenovo.

La explotación exitosa de las fallas podría permitir a un atacante deshabilitar las protecciones flash SPI o el Arranque seguro, otorgando efectivamente al adversario la capacidad de instalar malware persistente que puede sobrevivir a los reinicios del sistema.

CVE-2021-3970, por otro lado, se relaciona con un caso de corrupción de memoria en el Modo de administración del sistema de la firma, lo que llevó a la ejecución de código malicioso con los privilegios más altos.

Las tres fallas se informaron el 11 de octubre de 2021, luego de lo cual se emitieron parches el 12 de abril de 2022. A continuación, se muestra un resumen de las tres fallas descritas por Lenovo:

- CVE-2021-3970: una vulnerabilidad potencial en LenovoVariable SMI Handler debido a una validación insuficiente en algunos modelos de portátiles Lenovo puede permitir que un atacante con acceso local y privilegios elevados ejecute código arbitrario.
- CVE-2021-3971: una vulnerabilidad potencial de un controlador utilizado durante los procesos de fabricación más antiguos en algunos dispositivos portátiles Lenovo de consumo que se incluyó por error en la imagen del BIOS podría permitir que un atacante con privilegios elevados modifique la región de protección del firmware mediante la modificación de una variable NVRAM.
- CVE-2021-3972: una posible vulnerabilidad de un controlador utilizado durante el proceso de fabricación en algunos dispositivos portátiles Lenovo de consumo que no se desactivó por error puede permitir que un atacante con privilegios elevados modifique la configuración de arranque seguro modificando una variable NVRAM.

Remediación / Referencias

Recomendamos a todos los propietarios de computadoras portátiles Lenovo que revisen la lista de dispositivos afectados y actualicen su firmware, idealmente siguiendo las instrucciones del fabricante.

Por mayor información acceder a:
https://www.europapress.es/portaltic/ciberseguridad/noticia-descubren-vulnerabilidades-portatiles-lenovo-permiten-atacantes-ejecutar-malware-nivel-firmware-20220419172253.html

	**La aplicación para PC 7-Zip tiene una gran vulnerabilidad en Windows**	CRÍTICO

Descripción

Se ha descubierto una vulnerabilidad en la aplicación 7-Zip para Windows. Esto permitiría a un usuario local obtener un acceso de nivel superior.

Estado

Las herramientas de archivado de archivos como WinZip y WinRAR existen desde hace décadas y le permiten comprimir archivos para ahorrar espacio de almacenamiento y descomprimirlos cuando necesita acceder a los archivos en cuestión. Pero 7-Zip se convirtió en una de las herramientas de archivado de archivos más populares en los años posteriores a su lanzamiento debido a su soporte para una variedad de formatos zip.

Remediación / Referencias

Para abordar esta vulnerabilidad, se plantearon dos soluciones: el primer método es eliminar el archivo 7-zip.chm, mientras que la segunda forma es asegurarse de que 7-Zip solo tenga permisos de lectura y ejecución para todos los usuarios de la PC.

Por mayor información acceder a:
https://blog.segu-info.com.ar/2022/04/vulnerabilidad-en-7-zip-permite.html

Java	**Error en Java hace que las firmas digitales no tengan valor**	CRÍTICO

Descripción

Debido a un error en la implementación de firmas digitales, muchos entornos Java aceptan firmas digitales falsificadas.

Estado

El error afecta a las firmas digitales basadas en los Algoritmos de Firma Digital de Curva Elíptica (EDSA). Un poco simplificado, una firma digital consta de dos números enteros r y s, que junto con la clave involucrada deben satisfacer una ecuación para que la firma sea válida. Sin embargo, r y s no deben ser explícitamente 0, de lo contrario, las ecuaciones siempre dan como resultado el trivial "0 = 0" y, por lo tanto, una firma válida.

Sin embargo, los desarrolladores de Java olvidaron exactamente esta prueba para el valor sin sentido 0. Más específicamente, se quedó en el camino cuando portaron el código criptográfico JDK para Java 15 a Java; la versión anterior de C++ todavía lo contenía. Según el descubridor Neil Madden, las versiones de Java 15, 16, 17 y 18 anteriores a Critical Patch Update (CPU) en abril de 2022 se ven específicamente afectadas. Critical Patch Update, con el que Oracle eliminó la vulnerabilidad. Madden afirma haber informado sobre el error en noviembre del año pasado.

Las firmas digitales suelen estar destinadas a probar la autenticidad de cierta información y se utilizan en innumerables lugares en esta función: Prueba de identidad en forma de certificados, como firma digital bajo contratos u otros documentos, prueba de la autenticidad de paquetes de software, etc. y así sucesivamente. Si una aplicación Java basada en una de las bibliotecas afectadas completa una de estas tareas, los atacantes lo tienen fácil: pueden proporcionar cualquier dato con una firma vacía y la aplicación confirmará su autenticidad.

Remediación / Referencias

Cualquiera que use o desarrolle tales aplicaciones debe importar rápidamente la actualización Java actual de Oracle y proporcionar nuevas versiones de su software si es necesario.

Por mayor información acceder a: https://blog.segu-info.com.ar/2022/04/firmas-digitales-vacias-en-java-parchea.html

	Google lanza una actualización urgente de Chrome para una falla de día cero	PREVENCIÓN

Descripción

Google envió el jueves parches de emergencia para abordar dos problemas de seguridad en su navegador web Chrome, uno de los cuales dice que está siendo explotado activamente en la naturaleza.

Estado

Rastreado como CVE-2022-1364, el gigante tecnológico describió el error de alta gravedad como un caso de confusión de tipos en el motor JavaScript V8. A Clément Lecigne, del Grupo de análisis de amenazas de Google, se le atribuye la notificación de la falla el 13 de abril de 2022.

Como suele ser el caso con las fallas de día cero explotadas activamente, la compañía reconoció que está "consciente de que existe una vulnerabilidad para CVE-2022-1364". Se han retenido detalles adicionales sobre la falla y la identidad de los actores de la amenaza para evitar más abusos.

Con la última solución, Google ha parcheado un total de tres vulnerabilidades de día cero en Chrome desde principios de año. También es el segundo tipo de error relacionado con la confusión en V8 que se elimina en menos de un mes:

- CVE-2022-0609 - Use-after-free en Animación
- CVE-2022-1096 - Confusión de tipo en V8

Remediación / Referencias

Se recomienda a los usuarios que actualicen a la versión 100.0.4896.127 para Windows, macOS y Linux para frustrar posibles amenazas. También se recomienda a los usuarios de navegadores basados en Chromium como Microsoft Edge, Brave, Opera y Vivaldi que apliquen las correcciones a medida que estén disponibles.

Para saber más invitamos a visitar el siguiente sitio:
https://www.infobae.com/america/agencias/2022/04/07/google-lanza-actualizacion-de-emergencia-para-su-navegador-chrome-2/?outputType=amp-type

CISCO	**Error crítico en el software del controlador de LAN inalámbrica de Cisco**	PREVENCIÓN

Descripción

Cisco ha lanzado parches para contener una vulnerabilidad de seguridad crítica que afecta al controlador de LAN inalámbrica (WLC) que podría ser abusada por un atacante remoto no autenticado para tomar el control de un sistema afectado.

Estado

Registrado como CVE-2022-20695, el problema recibió una calificación de 10 sobre 10 en cuanto a gravedad y permite que un adversario omita los controles de autenticación e inicie sesión en el dispositivo a través de la interfaz de administración de WLC.

La explotación exitosa de la falla podría permitir que un atacante obtenga privilegios de administrador y lleve a cabo acciones maliciosas de una manera que permita tomar el control completo del sistema vulnerable.

La compañía enfatizó que el problema solo afecta a los siguientes productos si ejecutan la versión 8.10.151.0 o la versión 8.10.162.0 del software WLC de Cisco y tienen la compatibilidad con el radio de macfilter configurada como Otro:

- Controlador inalámbrico 3504
- Controlador inalámbrico 5520
- Controlador inalámbrico 8540
- Movilidad Express, y
- Controlador inalámbrico virtual (vWLC)

Remediación / Referencias

Se recomienda a los usuarios que actualicen a la versión 8.10.171.0 para corregir la falla. Las versiones 8.9 y anteriores de Cisco Wireless LAN Controller, así como la 8.10.142.0 y anteriores, no son vulnerables.

Para saber más invitamos a visitar el siguiente sitio:
https://blogs.masterhacks.net/noticias/hacking-y-ciberdelitos/vulnerabilidad-critica-de-omision-de-autenticacion-detectada-en-el-software-del-controlador-de-lan-inalambrica-de-cisco/

Conclusión

En esta nueva quincena de noticias destacamos vulnerabilidades de software que a nivel estratégico y general; las organizaciones deben de contar con inventarios del software y versiones utilizadas en sus ambientes, de tal forma de poder identificar y priorizar adecuadamente cuando nuevas vulnerabilidades son descubiertas sobre los mismos. De esta manera la rapidez en la implementación de los procesos de parcheo se acelera y además se crean hábitos de seguridad y actualizaciones periódicas en los sistemas que así lo requieran.

Mantener este seguimiento operativo es crucial frente a cómo trabajan y afectan las amenazas informáticas en la actualidad sobre entornos corporativos. Las mismas se aprovechan y difunden a través de estos problemas conocidos en software popular.

Nuestra principal recomendación es reducir los riesgos y vulnerabilidades a través de procesos diarios de actualizaciones de software dentro de todo el diverso entorno de software que utiliza una organización moderna. Por lo general esto es apoyado por diversos equipos tanto de seguridad, como de implementación de cambios, administradores de sistemas y demás colaboradores.

Apoyamos a las empresas a diferentes niveles para que puedan cumplir con estos objetivos de reducción de riesgos, y de gestionar sus vulnerabilidades informáticas actuales.

Manteniéndonos informados de las nuevas vulnerabilidades a través de nuestro boletín, podemos garantizar que la ventana de exposición de estas sea la menor posible, de tal forma de que la misma no genere impactos negativos.

Desde Datasec seguimos protegiendo sus activos más importantes. Nuestro equipo saluda una vez más a nuestros lectores, y hasta una nueva entrega de este boletín informativo de ciberseguridad.