Boletín de Ciberseguridad N°57

Fecha de publicación: 24/04/2023

Mes de abril

10/04/2023 – 24/04/2023

Datasec

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 segunda quincena del mes de abril se destacan 5 noticias de relevancia: 3 sobre vulnerabilidades tecnológicas, y 2 de prevención.

Aquellas noticias a tener especial recaudo son las siguientes:

CISA agrega 3 fallas explotadas activamente al catálogo de KEV

El viernes se agregaron tres fallas de seguridad al catálogo de Vulnerabilidades Explotadas Conocidas (KEV), según la evidencia de explotación activa.

Cisco y VMware lanzan actualizaciones de seguridad para corregir fallas críticas

Cisco y VMware han lanzado actualizaciones de seguridad para abordar fallas de seguridad críticas en sus productos que podrían ser aprovechadas por actores malintencionados para ejecutar código arbitrario en los sistemas afectados.

Google Chrome lanza actualización de parche urgente

Google lanzó el martes soluciones de emergencia para abordar otra falla de día cero de alta gravedad explotada activamente en su navegador web Chrome.

Vulnerabilidad Crítica

	CISA agrega 3 fallas explotadas activamente al catálogo de KEV	CRÍTICO

Descripción

El viernes se agregaron tres fallas de seguridad al catálogo de Vulnerabilidades Explotadas Conocidas (KEV), según la evidencia de explotación activa.

Estado

Las tres vulnerabilidades son las siguientes:

- CVE-2023-28432 (puntuación CVSS: 7,5): vulnerabilidad de divulgación de información de MinIO
- CVE-2023-27350 (puntuación CVSS: 9,8): vulnerabilidad de control de acceso inadecuado PaperCut MF/NG
- CVE-2023-2136 (puntuación CVSS - TBD): vulnerabilidad de desbordamiento de enteros de Google Chrome Skia

Los datos recopilados por GreyNoise muestran que hasta 18 direcciones IP maliciosas únicas de los EE. UU., los Países Bajos, Francia, Japón y Finlandia han intentado explotar la falla en los últimos 30 días.

La compañía de inteligencia de amenazas, en una alerta publicada a fines del mes pasado, también señaló cómo una implementación de referencia proporcionada por OpenAI para que los desarrolladores integren sus complementos en ChatGPT se basó en una versión anterior de MinIO que es vulnerable a CVE-2023-28432.

Remediación / Referencias

La vulnerabilidad se ha abordado a partir del 8 de marzo de 2023, con el lanzamiento de las versiones 20.1.7, 21.2.11 y 22.0.9 de PaperCut MF y PaperCut NG. Se espera que Zero Day Initiative, que informó el problema el 10 de enero de 2023, publique detalles técnicos adicionales el 10 de mayo de 2023.

Por mayor información acceder a:

https://nvd.nist.gov/vuln/detail/CVE-2023-28432

Falla de GhostToken que podría permitir a los atacantes ocultar aplicaciones maliciosas

CRÍTICO

Descripción

Se revelan detalles de una falla de día cero ahora parcheada en Google Cloud Platform (GCP) que podría haber permitido a los actores de amenazas ocultar una aplicación maliciosa inamovible dentro de la cuenta de Google de una víctima.

Estado

Apodado GhostToken por el startup israelí de ciberseguridad Astrix Security, la deficiencia afecta a todas las cuentas de Google, incluidas las cuentas de Workspace centradas en empresas. Se descubrió y se informó a Google el 19 de junio de 2022. La empresa implementó un parche global más de nueve meses después, el 7 de abril de 2023.

La falla hace posible que un atacante oculte su aplicación maliciosa de la página de administración de aplicaciones de la cuenta de Google de la víctima, lo que evita que los usuarios revoquen su acceso.

Esto se logra eliminando el proyecto de GCP asociado con la aplicación de OAuth autorizada, lo que hace que entre en un estado de "eliminación pendiente". El actor de amenazas, armado con esta capacidad, podría mostrar la aplicación no autorizada al restaurar el proyecto y usar el token de acceso para obtener los datos de la víctima y volverla invisible.

Remediación / Referencias

El parche de Google soluciona el problema y ahora también muestra las aplicaciones que están en un estado pendiente de eliminación en la página de acceso de terceros, lo que permite a los usuarios revocar el permiso otorgado a dichas aplicaciones.

Por mayor información acceder a:

https://nvd.nist.gov/vuln/detail/CVE-2023-28432

Goldoson Android Malware infecta más de 100 millones de descargas de Google Play Store

CRÍTICO

Descripción

Se detectó una nueva cepa de malware de Android llamada Goldoson en la tienda oficial de Google Play que abarca más de 60 aplicaciones legítimas que en conjunto tienen más de 100 millones de descargas.

Estado

Se han rastreado ocho millones de instalaciones adicionales a través de ONE store, una tienda líder de aplicaciones de terceros en Corea del Sur.

El componente no autorizado es parte de una biblioteca de software de terceros utilizada por las aplicaciones en cuestión y es capaz de recopilar información sobre las aplicaciones instaladas, los dispositivos conectados a Wi-Fi y Bluetooth y las ubicaciones de GPS.

Además, incluye la capacidad de cargar páginas web de forma sigilosa, una característica que podría abusarse para cargar anuncios con fines de lucro. Lo logra cargando código HTML en un WebView oculto y dirigiendo el tráfico a las URL.

Luego de la divulgación responsable a Google, 36 de las 63 aplicaciones infractoras se retiraron de Google Play Store. Las 27 aplicaciones restantes se han actualizado para eliminar la biblioteca maliciosa.

Los hallazgos resaltan la necesidad de que los desarrolladores de aplicaciones sean transparentes sobre las dependencias utilizadas en su software, sin mencionar que deben tomar las medidas adecuadas para proteger la información de los usuarios contra dicho abuso.

Remediación / Referencias

Se recomienda a los usuarios que solo descarguen aplicaciones de fuentes confiables, analicen los permisos de las aplicaciones, usen contraseñas seguras, habiliten la autenticación multifactor y tengan cuidado al recibir SMS o correos electrónicos de remitentes desconocidos.

Por mayor información acceder a:

https://nvd.nist.gov/vuln/detail/CVE-2023-28432

Prevención

CISCO	**Cisco y VMware lanzan actualizaciones de seguridad para corregir fallas críticas**	PREVENCIÓN

Descripción

Cisco y VMware han lanzado actualizaciones de seguridad para abordar fallas de seguridad críticas en sus productos que podrían ser aprovechadas por actores malintencionados para ejecutar código arbitrario en los sistemas afectados.

Estado

La más grave de las vulnerabilidades es una falla de inyección de comandos en Cisco Industrial Network director (CVE-2023-20036, puntaje CVSS: 9.9), que reside en el componente de la interfaz de usuario web y surge como resultado de una validación de entrada incorrecta al cargar un paquete de dispositivos.

Los parches están disponibles en la versión 1.11.3, y Cisco acredita a un investigador "externo" no identificado por informar los dos problemas.

Cisco también solucionó otra falla crítica en el mecanismo de autenticación externa de la plataforma de simulación de red de Modeling Labs. Registrada como CVE-2023-20154 (puntaje CVSS: 9.1), la vulnerabilidad podría permitir que un atacante remoto no autenticado acceda a la interfaz web con privilegios administrativos.

Remediación / Referencias

Cisco advierte a los clientes que prueben la efectividad de dichas soluciones en sus propios entornos antes de administrarlas. La deficiencia se corrigió con el lanzamiento de la versión 2.5.1

Por mayor información acceder a:

https://csirt.telconet.net/comunicacion/noticias-seguridad/cisco-y-vmware-lanzan-actualizaciones-de-seguridad-para-corregir-fallas-criticas-en-sus-productos/

	**Google Chrome lanza actualización de parche urgente**	PREVENCIÓN

Descripción

Google lanzó el martes soluciones de emergencia para abordar otra falla de día cero de alta gravedad explotada activamente en su navegador web Chrome.

Estado

La falla, rastreada como CVE-2023-2136, se describe como un caso de desbordamiento de enteros en Skia , una biblioteca de gráficos 2D de código abierto. A Clément Lecigne del Threat Analysis Group (TAG) de Google se le atribuye el descubrimiento y la notificación de la falla el 12 de abril de 2023.

El gigante tecnológico, que también solucionó otros siete problemas de seguridad con la última actualización, dijo que está al tanto de la explotación activa de la falla, pero no reveló detalles adicionales para evitar más abusos.

El desarrollo marca la segunda vulnerabilidad de día cero de Chrome en ser explotada por actores malintencionados este año, y se produce apenas unos días después de que Google parchó CVE-2023-2033 la semana pasada. No está claro de inmediato si los dos días cero se han encadenado como parte de ataques en estado salvaje.

Remediación / Referencias

Se recomienda a los usuarios actualizar a la versión 112.0.5615.137/138 para Windows, 112.0.5615.137 para macOS y 112.0.5615.165 para Linux para mitigar 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.

Por mayor información acceder a:

https://nvd.nist.gov/vuln/detail/CVE-2023-2136

Conclusiones

En esta segunda quincena de abril, destacamos cinco noticias importantes, tres sobre vulnerabilidades tecnológicas y dos sobre prevención.

Se destacan noticias como las tres vulnerabilidades recientemente agregadas al catálogo de vulnerabilidades conocidas (KEV) por CISA, la actualización de seguridad lanzada por Cisco y VMware, y la actualización de parche urgente lanzada por Google Chrome. Además, se proporciona información detallada sobre cada vulnerabilidad, incluyendo su estado y referencias para su remediación.

Se incluyen detalles sobre una vulnerabilidad de día cero ahora parcheada en Google Cloud Platform (GCP) que podría haber permitido a los actores de amenazas ocultar una aplicación maliciosa inamovible dentro de la cuenta de Google de una víctima.

Se proporcionan detalles sobre el estado de estas debilidades y cómo podríamos prevenirlas y remediarlas correspondiente.