Boletín de Ciberseguridad N°80

Fecha de publicación: 31/05/2024

09/05/2024 – 30/05/2024

Datasec

BOLETÍN DE CIBERSEGURIDAD

Indice

Introducción

En otra edición de nuestro boletín de ciberseguridad, acercamos las alertas y noticias destacadas de la última quincena en materia de ciberseguridad. En este sentido, incluimos además varias noticias vinculadas a la prevención de riesgos, lo cual configura uno de los ejes fundamentales en la madurez de una organización en cuanto a su ciberseguridad.

Nuestro servicio de monitoreo 24/7 SOC (Centro de Operaciones de Seguridad) es justamente uno de nuestros principales servicios, entendiendo que configura un componente crítico de cualquier estrategia de protección. A través de este servicio, proporcionamos una ubicación centralizada para el análisis continuo de amenazas, detección y respuesta, para prevenir incidentes de ciberseguridad.

Vulnerabilidad Crítica

	**Vulnerabilidad de día cero en Google Chrome (CVE-2024-4997) explota activamente**	CRÍTICO

Descripción

Google ha lanzado una actualización de seguridad de emergencia para su navegador web Chrome para corregir una vulnerabilidad de alta gravedad que está siendo explotada activamente por atacantes.

La falla de día cero, rastreada como CVE-2024-4947, es un error de confusión de tipos en el motor JavaScript V8 que podría permitir ataques de ejecución remota de código.

Un error de confusión de tipos en el motor JavaScript V8 se refiere a una vulnerabilidad donde el motor interpreta incorrectamente el tipo de un objeto, lo que lleva a errores lógicos y potencialmente permite a los atacantes ejecutar código arbitrario.

Este tipo de vulnerabilidad es particularmente peligrosa porque puede ser explotada para causar corrupción de la memoria heap mediante la creación de una página HTML específica que desencadene el error, comprometiendo así la seguridad del navegador y del sistema subyacente.

Chrome 125.0.6422.60 para Linux y 125.0.6422.60/.61 para Windows y Mac traen varias correcciones y mejoras al popular navegador web. El registro de lanzamientos oficial proporciona una lista completa de los cambios.

Estado: Crítico

Remediación:

Los investigadores de seguridad Vasily Berdnikov y Boris Larin de Kaspersky descubrieron la vulnerabilidad el 13 de mayo y la reportaron a Google.

"Google es consciente de un exploit para CVE-2024-4947 y urge a los usuarios a actualizar sus navegadores lo antes posible."

Si bien Chrome se actualizará automáticamente para la mayoría de los usuarios, Google insta a todos los usuarios de Chrome en Windows, Mac y Linux a asegurarse de que están ejecutando la versión 125.0.6422.60 o posterior verificando manualmente las actualizaciones.

Otras correcciones de seguridad Además del parche de día cero, la actualización de Chrome 125 incluye otras 8 correcciones de seguridad:

- CVE-2024-4948 (Alta) – Uso después de liberación en Dawn, reportado por wgslfuzz

- CVE-2024-4949 (Media) – Uso después de liberación en V8, reportado por Ganjiang Zhou
- CVE-2024-4950 (Baja) – Implementación inapropiada en Descargas, reportado por Shaheen Fazim
- Varias otras correcciones de auditorías internas y fuzzing

Google ha restringido el acceso a los detalles de los errores hasta que la mayoría de los usuarios hayan actualizado Chrome. La compañía agradeció a todos los investigadores externos, así como a sus equipos de seguridad internos, por sus contribuciones a esta versión.

Por mayor información acceder a:

https://cybersecuritynews-com.cdn.ampproject.org/c/s/cybersecuritynews.com/google-chrome-zero-day-vulnerability/amp/

VEEAM	**Vulnerabilidades críticas en Veeam**	CRÍTICO

Descripción

Veeam advierte a sus clientes que parcheen una **vulnerabilidad de seguridad crítica** que permite a atacantes no autenticados iniciar sesión en cualquier cuenta a través de Veeam Backup Enterprise Manager (VBEM). El error, identificado como CVE-2024-29849 (CVSS de 9,8/10) "permite a un atacante no autenticado iniciar sesión en la interfaz web de Veeam Backup Enterprise Manager como cualquier usuario", explica la empresa.

Estado: crítico

Remediación:

Los administradores que no pueden actualizar inmediatamente a VBEM versión 12.1.2.172, que corrige esta falla de seguridad, aún pueden mitigarla deteniendo y deshabilitando los servicios VeeamEnterpriseManagerSvc (Veeam Backup Enterprise Manager) y VeeamRESTSvc (Veeam RESTful API). Veeam también parcheó otras dos vulnerabilidades VBEM de alta gravedad, una que permite la apropiación de cuentas a través de retransmisión NTLM (CVE-2024-29850) y una segunda que permite a usuarios con altos privilegios robar el hash NTLM de la cuenta de servicio Veeam Backup Enterprise Manager si es no configurado para ejecutarse como la cuenta predeterminada del sistema local (CVE-2024-29851).

Se han parcheado las siguientes vulnerabilidades en Veeam Backup Enterprise Manager (VBEM):

- CVE-2024-29849 (Crítica (9,8): esta vulnerabilidad permite que un atacante no autenticado inicie sesión en la interfaz web de Veeam Backup Enterprise Manager como cualquier usuario.
- CVE-2024-29850 (Alta 8,8): esta vulnerabilidad permite la toma de cuentas a través de retransmisión NTLM.
- CVE-2024-29851 (Alta 7,2): esta vulnerabilidad permite a un usuario con altos privilegios robar el hash NTLM de la cuenta de servicio de Veeam Backup Enterprise Manager si esa cuenta de servicio no es la cuenta predeterminada del sistema local.
- CVE-2024-29852 (Baja 2,7): esta vulnerabilidad permite a los usuarios con altos privilegios leer registros de sesiones de respaldo. Veeam Agent para Windows (VAW).

CVE-2024-29853 (Alta 7,8): esta vulnerabilidad en Veeam Agent para Microsoft Windows permite el escalamiento de privilegios locales.

Por mayor información acceder a:
https://blog.segu-info.com.ar/2024/05/vulnerabilidades-criticas-en-veeam.html

Prevención

DNSBomb: Nuevo ataque DOS práctico y potente

PREVENCIÓN

Descripción:

DNS emplea una variedad de mecanismos para garantizar la disponibilidad, proteger la seguridad y mejorar la confiabilidad. Sin embargo, en este paper investigadores de la Universidad Tsinghua de Pekín, revelan que estos mecanismos inherentes, incluidos el tiempo de espera, la agregación de consultas y la respuesta rápida, pueden transformarse en vectores de ataque maliciosos; y proponen un nuevo ataque DoS denominado DNSBomb [PDF / Github].

DNSBomb explota múltiples mecanismos de DNS ampliamente implementados para acumular consultas de DNS que se envían a baja velocidad, para amplificar las consultas en respuestas de gran tamaño y concentrar todas las respuestas de DNS en una ráfaga de pulsaciones periódicas, cortas y de gran volumen para saturar simultáneamente los sistemas de destino.

A través de una evaluación exhaustiva de 10 software de DNS convencionales, 46 servicios de DNS públicos y alrededor de 1,8 millones de solucionadores de DNS abiertos, la investigación demuestra que todos estos podrían explotarse para llevar a cabo ataques DNSBomb más prácticos y potentes que los ataques DoS conocidos anteriormente.

Experimentos a pequeña escala muestran que la magnitud máxima del pulso puede acercarse a 8,7 Gb/s y el factor de amplificación del ancho de banda podría superar las 20.000 veces. Los ataques controlados realizados provocan la pérdida total de paquetes o la degradación del servicio en conexiones con y sin estado (TCP, UDP y QUIC).

El paper además, presenta soluciones de mitigación efectivas con evaluaciones detalladas y los investigadores informaron responsablemente sus hallazgos a todos los proveedores afectados y recibieron el reconocimiento de 24 de ellos, los cuales están parcheando su software utilizando las soluciones planteadas.

Por mayor información acceder a:

https://blog.segu-info.com.ar/2024/05/dnsbomb-nuevo-ataque-dos-practico-y.html

El troyano bancario Grandoreiro vuelve más fuerte que nunca

PREVENCIÓN

Descripción:

Los actores de amenazas detrás del troyano bancario Grandoreiro basado en Windows han regresado en una campaña global desde marzo de 2024, luego de una eliminación policial en enero.

- Grandoreiro es un troyano bancario multicomponente que funciona como malware como servicio (MaaS).
- Se utiliza activamente en campañas de phishing haciéndose pasar por entidades gubernamentales en México, Argentina y Sudáfrica.
- El troyano bancario se dirige específicamente a más de 1.500 aplicaciones y sitios web bancarios globales en más de 60 países, incluidas regiones de América Central y del Sur, África, Europa y el Indo-Pacífico.
- La última variante contiene actualizaciones importantes que incluyen descifrado de cadenas y cálculo DGA, lo que permite al menos 12 dominios C2 diferentes por día.
- Grandoreiro admite la recopilación de direcciones de correo electrónico de hosts infectados y el uso de su cliente Microsoft Outlook para enviar más campañas de phishing.

Según el nuevo informe de IBM X-Force, si bien Grandoreiro es conocido principalmente por su enfoque en América Latina, España y Portugal, la expansión probablemente sea un cambio de estrategia después de los intentos de las autoridades brasileñas de cerrar su infraestructura.

Desde marzo de 2024, X-Force ha observado campañas de phishing haciéndose pasar por el Servicio de Administración Tributaria (SAT) de México, la Comisión Federal de Electricidad (CFE) de México, la Secretaría de Administración y Finanzas de la Ciudad de México y el Servicio de Impuestos AFIP de Argentina. Los correos electrónicos están dirigidos a usuarios de América Latina, incluidos dominios de nivel superior (TLD) de México, Colombia y Chile *".mx", ".co", ".ar"* y *".cl"*.

Los ataques comienzan con correos electrónicos de phishing que instruyen a los destinatarios a hacer clic en un enlace para ver una factura o realizar un pago, según la naturaleza del señuelo y la entidad gubernamental suplantada en los mensajes. Los usuarios que terminan haciendo clic en el enlace son redirigidos a una imagen de un ícono de PDF, lo que finalmente conduce a la descarga de un archivo ZIP con el ejecutable del cargador Grandoreiro.

El cargador personalizado se "infla" artificialmente a más de 100 MB para evitar el software de escaneo antimalware. También es responsable de garantizar que el host comprometido no se encuentre en un entorno aislado, recopilar datos básicos de la víctima en un servidor de comando y control (C2) y descargar y ejecutar el principal troyano bancario. Para eludir la ejecución automatizada, muestra una pequeña ventana emergente CAPTCHA que imita al lector de PDF de Adobe, el cual requiere un clic para continuar con la ejecución.

El cargador personalizado se "infla" artificialmente a más de 100 MB para evitar el software de escaneo antimalware. También es responsable de garantizar que el host comprometido no se encuentre en un entorno aislado, recopilar datos básicos de la víctima en un servidor de comando y control (C2) y descargar y ejecutar el principal troyano bancario. Para eludir la ejecución automatizada, muestra una pequeña ventana emergente CAPTCHA que imita al lector de PDF de Adobe, el cual requiere un clic para continuar con la ejecución.

Vale la pena señalar que el paso de verificación también se realiza para omitir sistemas geolocalizados en Rusia, Chequia, Polonia y los Países Bajos, así como máquinas con Windows 7 basadas en los EE.UU. sin antivirus instalado.

El componente troyano comienza su ejecución estableciendo persistencia a través del Registro de Windows, después de lo cual emplea un DGA rediseñado para establecer conexiones con un servidor C2 para recibir más instrucciones.

Grandoreiro admite una variedad de comandos que permiten a los actores de amenazas controlar remotamente el sistema, realizar operaciones con archivos y habilitar modos especiales, incluido un nuevo módulo que recopila datos de Microsoft Outlook y abusa de la cuenta de correo electrónico de la víctima para enviar mensajes de spam a otros objetivos.

"Para interactuar con el cliente Outlook local, Grandoreiro utiliza la herramienta Outlook Security Manager, un software utilizado para desarrollar complementos de Outlook. La razón principal detrás de esto es que Outlook Object Model Guard activa alertas de seguridad si detecta acceso a objetos protegidos".

Al utilizar el cliente Outlook local para enviar spam, Grandoreiro puede propagarse a través de las bandejas de entrada de las víctimas infectadas a través del correo electrónico, lo que probablemente contribuye a la gran cantidad de volumen de spam observado en Grandoreiro.

Por mayor información acceder a:

https://blog.segu-info.com.ar/2024/05/grandoreiro-vuelve-mas-fuerte-que-nunca.html

Novedades

wazuh.	**Datasec y Wazuh lanzan su webinar: fortaleciendo la ciberseguridad de las empresas uruguayas**	NOVEDADES

En el marco de nuestra colaboración con Wazuh, el próximo 5 de junio, 12 PM (UY-ARG) estaremos compartiendo nuestra experiencia de trabajo conjunto a través de un Webinar gratuito, brindando herramientas a todos quienes deseen integrar Wazuh a su ecosistema de ciberseguridad.

Comenzaremos destacando algunos de los hallazgos del Informe de Ciberseguridad de las Empresas Uruguayas realizado en conjunto con Grupo Radar, que da cuenta de las vulnerabilidades y desafíos que atraviesan hoy en día.

Por su parte, Wazuh compartirá el funcionamiento de esta plataforma de código abierto que permite adaptar las medidas de seguridad específicas de cada cliente y se ha convertido en una herramienta fundamental para nuestro servicio de monitoreo 24/7 (SOC).

Inscribite para participar en el webinar haciendo clic aquí.

VMWare Workstation Pro y Fusion Pro gratuitos para uso personal

NOVEDADES

VMWare ha hecho que Workstation Pro y Fusion Pro sean gratuitos para uso personal, lo que permite a los usuarios domésticos y a los estudiantes configurar sus propios laboratorios de pruebas virtualizados y jugar con otro sistema operativo por poco o ningún costo.

"La parte más interesante es que Fusion Pro y Workstation Pro ahora tendrán dos modelos de licencia. Ahora ofrecemos una suscripción de uso personal gratuito o una suscripción de uso comercial de pago para nuestras aplicaciones Pro", explica Michael Roy, gerente de producto para productos de hipervisor.

"Los usuarios decidirán en función de su caso de uso si se requiere una suscripción comercial. Esto significa que los usuarios cotidianos que quieran un laboratorio virtual en su computadora Mac, Windows o Linux pueden hacerlo de forma gratuita simplemente registrándose y descargandolos desde support.broadcom.com"

Después de registrar una cuenta de VMware e instalar Workstation Pro o Fusion, aparecerá una pantalla que le preguntará si utiliza el producto para uso personal o en un entorno comercial. Para usuarios personales, simplemente pueden seleccionar esa opción y se instalará con todas sus funciones estándar sin limitaciones.

Ahora que sus productos con todas las funciones son gratuitos, VMware dice que van a descontinuar Workstation Player y Fusion Player, y que ya no están disponibles para su compra. Para quienes utilizan productos VMware Player, la empresa ha proporcionado instrucciones sobre cómo actualizar a las versiones Pro.

Por más información acceder a:

https://blog.segu-info.com.ar/2024/05/vmware-workstation-pro-y-fusion-pro.html

Google: Llaves de acceso y protección entre cuentas

NOVEDADES

Para el Día Mundial de la Contraseña, Google compartió actualizaciones sobre las llaves de acceso en sus productos.

Las contraseñas suelen ser el núcleo de los principales problemas de ciberseguridad actuales, por lo que han seguido creando nuevas tecnologías de autenticación a lo largo de los años. En 2022, para el Día Mundial de la Contraseña, lanzaron las llaves de acceso. Desde entonces se han utilizado para autenticar usuarios más de 1,000 millones de veces en más de 400 millones de cuentas de Google.

Las llaves de acceso son fáciles de usar y resistentes al phishing, ya que solo requieren una huella dactilar, un escaneo facial o un pin, lo que las hace un 50% más rápidas que las contraseñas. De hecho, diariamente, las llaves de acceso ya se utilizan para la autenticación en cuentas de Google con más frecuencia que las formas heredadas de verificación en dos pasos (2SV), como las contraseñas de un solo uso (OTP) por SMS y las OTP basadas en aplicaciones (como las aplicaciones Authenticator) combinadas.

También anunciaron su programa de Protección entre cuentas y nuevas actualizaciones para las llaves de acceso.

Por mayor información acceder a:

https://blog.google/technology/safety-security/google-passkeys-update-april-2024/

Conclusiones

Finalizando mayo, el mes donde se celebra el Día Mundial de la Contraseña, vemos como Google, por ejemplo, fortaleció sus tecnologías de autenticación con el fin de brindar mayor seguridad a sus usuarios, entendiendo que las contraseñas son un núcleo principal de amenazas.

La ciberseguridad está marcada por la necesidad de una actualización constante así como una concientización tanto de las empresas como de los usuarios finales. En este sentido, con el fin de seguir capacitando y brindando herramientas para el monitoreo y prevención, es que nos encontramos trabajando fuertemente con nuestro Partner Platino Wazuh, de manera que más organizaciones conozcan su potencial. En junio, brindaremos un webinar gratuito, para que toda la región y nuestra comunidad digital pueda acceder a una instancia única con expertos que evacuarán todas las dudas sobre el referente en ciberseguridad de código abierto.

¡Hasta la próxima edición!