Boletín de Ciberseguridad N°74

Fecha de publicación: 22/01/2024

Mes de enero

08/01/2024 – 22/01/2024

Datasec

BOLETÍN DE CIBERSEGURIDAD

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 enero se destacan 6 noticias de relevancia, siendo estas sobre vulnerabilidades tecnológicas.

Aquellas noticias a tener especial recaudo son las siguientes:

CISA advierte zero day

CISA emite una directiva de emergencia a las agencias federales sobre las hazañas de día cero de Ivanti.

Campaña de malvertising utilizando Google Ads

Ciberdelincuentes malintencionados utilizan anuncios de Google para dirigirse a usuarios que buscan software popular.

Vulneración de correos electrónicos de Microsoft

Correos electrónicos de los principales ejecutivos de Microsoft fueron violados en un sofisticado ataque APT.

Vulnerabilidad Crítica

	CISA advierte zero day	CRÍTICO

Descripción

CISA emite una directiva de emergencia a las agencias federales sobre las hazañas de día cero de Ivanti.

Estado

La Agencia de Seguridad de Infraestructura y Ciberseguridad de EE. UU. (CISA) emitió el viernes una directiva de emergencia instando a implementar mitigaciones contra dos fallas de día cero explotadas activamente en Ivanti Connect Secure (ICS) e Ivanti Policy Secure (IPS).

El desarrollo llega cuando las vulnerabilidades (una omisión de autenticación y un error de inyección de código) han sido objeto de una explotación generalizada por parte de múltiples actores de amenazas. Las fallas permiten que un actor malintencionado cree solicitudes maliciosas y ejecute comandos arbitrarios en el sistema.

La compañía estadounidense reconoció en un aviso que ha sido testigo de un "fuerte aumento en la actividad de los actores de amenazas" a partir del 11 de enero de 2024, después de que se revelaran públicamente las deficiencias.

"La explotación exitosa de las vulnerabilidades en estos productos afectados permite que un actor de amenazas maliciosas se mueva lateralmente, realice una filtración de datos y establezca un acceso persistente al sistema, lo que resulta en un compromiso total de los sistemas de información objetivo", dijo la agencia.

Ivanti, que se espera que lance una actualización para abordar las fallas la próxima semana, ha puesto a disposición una solución temporal a través de un archivo XML que se puede importar a los productos afectados para realizar los cambios de configuración necesarios.

CISA insta a las organizaciones que ejecutan ICS a aplicar la mitigación y ejecutar una herramienta de verificación de integridad externa para identificar signos de compromiso y, si los encuentra, desconectarlos de las redes y restablecer el dispositivo, seguido de importar el archivo XML.

Además, se insta a las entidades FCEB a revocar y volver a emitir cualquier certificado almacenado, restablecer la contraseña de habilitación del administrador, almacenar claves API y restablecer las contraseñas de cualquier usuario local definido en la puerta de enlace.

Investigadores de ciberseguridad han observado ataques que utilizan las fallas gemelas como arma para implementar shells web y puertas traseras pasivas para el acceso persistente a dispositivos infectados. Se estima que hasta la fecha hasta 2.100 dispositivos en todo el mundo se han visto comprometidos.

Remediación / Referencias

Por mayor información acceder a:

https://www.cisa.gov/news-events/directives/ed-24-01-mitigate-ivanti-connect-secure-and-ivanti-policy-secure-vulnerabilities

https://forums.ivanti.com/s/article/Recovery-Steps-Related-to-CVE-2023-46805-and-CVE-2024-21887?language=en_US

Microsoft	Vulneración de correos electrónicos de Microsoft	CRÍTICO

Descripción

Correos electrónicos de los principales ejecutivos de Microsoft fueron violados en un sofisticado ataque APT.

Estado

Microsoft reveló que fue el objetivo de un ataque estado-nación a sus sistemas corporativos que resultó en el robo de correos electrónicos y archivos adjuntos de altos ejecutivos y otras personas en los departamentos legales y de ciberseguridad de la compañía.

El fabricante de Windows atribuyó el ataque a un grupo ruso de amenazas persistentes avanzadas (APT) que rastrea como Midnight Blizzard (anteriormente Nobelium), que también se conoce como APT29, BlueBravo, Cloaked Ursa, Cozy Bear y The Dukes.

Informó además que inmediatamente tomó medidas para investigar, interrumpir y mitigar la actividad maliciosa tras su descubrimiento.

“El actor de la amenaza utilizó un ataque de pulverización de contraseñas para comprometer una cuenta heredada de inquilino de prueba que no era de producción y ganar terreno, y luego utilizó los permisos de la cuenta para acceder a un porcentaje muy pequeño de las cuentas de correo electrónico corporativas de Microsoft, incluidos los miembros de nuestro equipo de liderazgo senior y empleados en nuestras funciones de ciberseguridad, legales y otras, y exfiltró algunos correos electrónicos y documentos adjuntos", dijo Microsoft.

La naturaleza del objetivo indica que los actores de la amenaza buscaban acceder a información relacionada con ellos mismos. También enfatizó que el ataque no fue el resultado de ninguna vulnerabilidad de seguridad en sus productos y que no hay evidencia de que el adversario haya accedido a entornos de clientes, sistemas de producción, código fuente o sistemas de inteligencia artificial.

El gigante informático, sin embargo, no reveló cuántas cuentas de correo electrónico fueron infiltradas ni a qué información se accedió, pero dijo que se trataba del proceso de notificar a los empleados que se vieron afectados como resultado del incidente.

El equipo de piratería, que anteriormente fue responsable del sonado compromiso de la cadena de suministro de SolarWinds, ha señalado a Microsoft dos veces, una en diciembre de 2020 por desviar el código fuente relacionado con los componentes de Azure, Intune y Exchange, y la segunda vez por vulnerar tres de sus clientes en junio de 2021 mediante pulverización de contraseñas y ataques de fuerza bruta.

"Este ataque resalta el riesgo continuo que representan para todas las organizaciones los actores de amenazas de estados-nación con buenos recursos como Midnight Blizzard", dijo el Centro de Respuesta de Seguridad de Microsoft (MSRC).

Remediación / Referencias

Por mayor información acceder a:

https://msrc.microsoft.com/blog/2024/01/microsoft-actions-following-attack-by-nation-state-actor-midnight-blizzard/

https://thehackernews.com/2024/01/microsofts-top-execs-emails-breached-in.html

APACHE ACTIVEMQ	Alerta: Fallo de Apache ActiveMQ	CRÍTICO

Descripción

Fallo de Apache ActiveMQ explotado en nuevos ataques de Godzilla Web Shell

Estado

Investigadores de ciberseguridad advierten sobre un "aumento notable" en la actividad de los actores de amenazas que explotan activamente una falla ahora parcheada en Apache ActiveMQ para entregar el shell web Godzilla en hosts comprometidos.

"Los web shells están ocultos dentro de un formato binario desconocido y están diseñados para evadir la seguridad y los escáneres basados en firmas". "En particular, a pesar del formato de archivo desconocido del binario, el motor JSP de ActiveMQ continúa compilando y ejecutando el shell web".

Con una puntuación CVSS de 10.0, hace referencia a una vulnerabilidad grave en Apache ActiveMQ que permite la ejecución remota de código. Desde su divulgación pública a finales de octubre de 2023, ha sido objeto de explotación activa por parte de múltiples

adversarios para implementar ransomware, rootkits, mineros de criptomonedas y botnets DDoS.

En el último conjunto de intrusiones observado, las instancias susceptibles han sido atacadas por shells web basados en JSP que se encuentran dentro de la carpeta "admin" del directorio de instalación de ActiveMQ.

El webshell, llamado Godzilla, es una puerta trasera rica en funciones capaz de analizar solicitudes HTTP POST entrantes, ejecutar el contenido y devolver los resultados en forma de respuesta HTTP.

"Lo que hace que estos archivos maliciosos sean particularmente notables es cómo el código JSP parece estar oculto dentro de un tipo desconocido de binario", dijeron investigadores de seguridad. "Este método tiene el potencial de eludir las medidas de seguridad, evadiendo la detección por parte de los puntos finales de seguridad durante el escaneo".

Un examen más detallado de la cadena de ataque muestra que el código del shell web se convierte en código Java antes de su ejecución por parte del Jetty Servlet Engine.

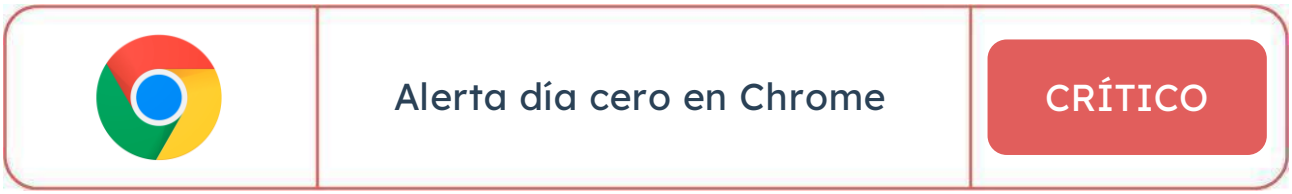
En última instancia, la carga útil JSP permite al actor de amenazas conectarse al shell web a través de la interfaz de usuario de administración de Godzilla y obtener un control completo sobre el host de destino, lo que facilita la ejecución de comandos de shell arbitrarios, la visualización de información de la red y el manejo de operaciones de administración de archivos.

Remediación / Referencias

Se recomienda encarecidamente a los usuarios de Apache ActiveMQ que actualicen a la última versión lo antes posible para mitigar posibles amenazas.

Por mayor información acceder a:

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-46604



Descripción

Alerta de día cero: actualice Chrome ahora para corregir una nueva vulnerabilidad explotada activamente.

Estado

Google lanzó actualizaciones para solucionar cuatro problemas de seguridad en su navegador Chrome, incluida una falla de día cero explotada activamente.

Se refiere a un acceso a la memoria fuera de los límites en el motor V8 JavaScript y WebAssembly, que los actores de amenazas pueden utilizar como arma para provocar un bloqueo.

"Al leer la memoria fuera de los límites, un atacante podría obtener valores secretos, como direcciones de memoria, que pueden evitar mecanismos de protección como ASLR para mejorar la confiabilidad y la probabilidad de explotar una debilidad separada para lograr el código ejecución en lugar de simplemente denegación de servicio", según la Enumeración de Debilidades Comunes (CWE) de MITRE.

Se han ocultado detalles adicionales sobre la naturaleza de los ataques y los actores de amenazas que pueden estar explotándolos en un intento de evitar una mayor explotación. El problema se informó de forma anónima el 11 de enero de 2024.

"El acceso a la memoria fuera de los límites en V8 en Google Chrome antes de 120.0.6099.224 permitía a un atacante remoto explotar potencialmente la corrupción del montón a través de una página HTML diseñada", se lee en una descripción de la falla en la Base de datos nacional de vulnerabilidad (NVD) del NIST.

El desarrollo marca el primer día cero explotado activamente que Google parcheará en Chrome en 2024. El año pasado, el gigante tecnológico resolvió un total de 8 días cero explotados activamente en el navegador.

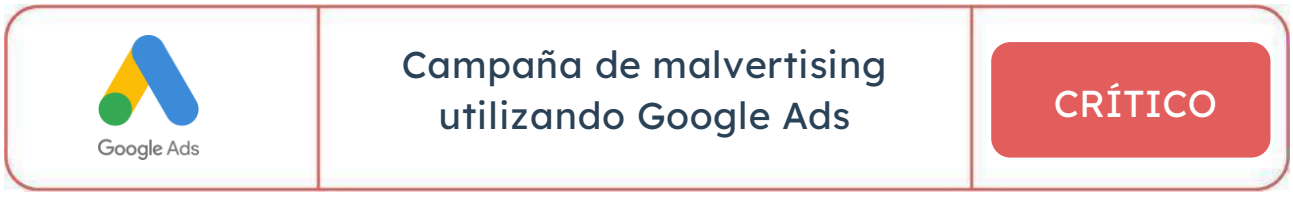
Remediación / Referencias

Se recomienda a los usuarios actualizar a la versión 120.0.6099.224/225 de Chrome para Windows, 120.0.6099.234 para macOS y 120.0.6099.224 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 cuando estén disponibles.

Por mayor información acceder a:

https://chromereleases.googleblog.com/2024/01/stable-channel-update-for-desktop_16.html



Descripción

Ciberdelincuentes malintencionados utilizan anuncios de Google para dirigirse a usuarios que buscan software popular.

Estado

Han surgido detalles sobre una campaña de publicidad maliciosa que aprovecha Google Ads para dirigir a los usuarios que buscan software popular a páginas de destino ficticias y distribuir cargas útiles de la siguiente etapa.

Investigadores, quienes descubrieron la actividad, informaron que es "única en su forma de tomar huellas dactilares de los usuarios y distribuir cargas útiles urgentes".

El ataque señala a los usuarios que buscan convertidores Notepad++ y PDF para publicar anuncios falsos en la página de resultados de búsqueda de Google que, al hacer clic en ellos, filtra los bots y otras direcciones IP no deseadas mostrando un sitio señuelo.

Si se considera que el visitante es de interés para el actor de la amenaza, la víctima es redirigida a un sitio web réplica que anuncia el software, mientras toma silenciosamente las huellas dactilares del sistema para determinar si la solicitud se origina en una máquina virtual.

Los usuarios que no pasan la verificación son dirigidos al sitio web legítimo de Notepad++, mientras que a un objetivo potencial se le asigna una identificación única para "fines de seguimiento, pero también para hacer que cada descarga sea única y urgente".

El malware de etapa final es una carga útil HTA que establece una conexión a un dominio remoto ("mybigeye[.]icu") en un puerto personalizado y sirve malware de seguimiento.

"Los actores de amenazas están aplicando con éxito técnicas de evasión que eluden los controles de verificación de anuncios y les permiten apuntar a ciertos tipos de víctimas", comentan investigadores.

"Con una cadena de entrega de malware confiable, los actores maliciosos pueden concentrarse en mejorar sus páginas señuelo y crear cargas útiles de malware personalizadas".

La divulgación se superpone con una campaña similar dirigida a los usuarios que buscan el administrador de contraseñas KeePass con anuncios maliciosos que dirigen a las víctimas a un dominio que usa Punycode (keepass[.]info vs. ķeepass[.]info), una codificación especial utilizada para convertir caracteres Unicode a ASCII.

Las personas que hagan clic en el anuncio serán redirigidas a través de un servicio de encubrimiento destinado a filtrar zonas de pruebas, bots y cualquier persona que no se considere una víctima genuina. Los actores de amenazas han configurado un dominio temporal en el sitio keepastacking[.] que realiza la redirección condicional al destino final.

Los usuarios que llegan al sitio señuelo son engañados para que descarguen un instalador malicioso que, en última instancia, conduce a la ejecución de FakeBat (también conocido como EugenLoader), un cargador diseñado para descargar otro código malicioso.

El abuso de Punycode no es del todo novedoso, pero combinarlo con Google Ads deshonestos es una señal de que la publicidad maliciosa a través de los motores de búsqueda se está volviendo más sofisticada. Al emplear Punycode para registrar nombres

de dominio similares como un sitio legítimo, el objetivo es realizar un ataque homógrafo y atraer a las víctimas para que instalen malware.

"Si bien los actores de amenazas han utilizado Punycode con nombres de dominio internacionalizados durante años para atacar a las víctimas de phishing, esto demuestra cuán efectivo sigue siendo en el contexto de la suplantación de marcas a través de publicidad maliciosa", informan los expertos.

Remediación / Referencias

Por mayor información acceder a:

https://thehackernews.com/2023/10/malvertisers-using-google-ads-to-target.html

Emerge nuevo grupo de ransomware

CRÍTICO

Descripción

Surge un nuevo grupo de ransomware con la infraestructura y el código fuente de Hive.

Estado

Los actores de amenazas detrás de un nuevo grupo de ransomware llamado Hunters International han adquirido el código fuente y la infraestructura de la operación Hive ahora desmantelada para impulsar sus propios esfuerzos en el panorama de amenazas.

"Parece que el liderazgo del grupo Hive tomó la decisión estratégica de cesar sus operaciones y transferir sus activos restantes a otro grupo, Hunters International", informó el director de soluciones técnicas de Bitdefender, en un informe publicado la semana pasada.

Hive, que alguna vez fue una prolífica operación de ransomware como servicio (RaaS), fue eliminado como parte de una operación policial coordinada en enero de 2023.

Si bien es común que los actores de ransomware se reagrupen, cambien el nombre o disuelvan sus actividades después de tales incautaciones, lo que también puede suceder es que los desarrolladores principales puedan pasar el código fuente y otra infraestructura en su poder a otro actor de amenazas.

Los informes sobre Hunters International como un posible cambio de marca de Hive surgieron el mes pasado después de que se identificaran varias similitudes de código entre las dos cepas. Desde entonces se ha cobrado cinco víctimas hasta la fecha.

Sin embargo, los actores de amenazas detrás de esto han tratado de disipar estas especulaciones, afirmando que compraron el código fuente y el sitio web de Hive a sus desarrolladores.

"El grupo parece poner mayor énfasis en la filtración de datos". "En particular, a todas las víctimas reportadas se les extrajeron datos, pero no a todas se les cifraron", lo que convierte a Hunters International en una organización de extorsión de datos.

El análisis de Bitdefender de la muestra de ransomware revela sus fundamentos basados en Rust, un hecho confirmado por la transición de Hive al lenguaje de programación en julio de 2022 por su mayor resistencia a la ingeniería inversa.

"En general, a medida que el nuevo grupo adopta este código de ransomware, parece que han apuntado a la simplificación", dijo el Director.

Han reducido el número de parámetros de la línea de comandos, han simplificado el proceso de almacenamiento de claves de cifrado y han hecho que el malware sea menos detallado en comparación con versiones anteriores.

El ransomware, además de incorporar una lista de exclusión de extensiones de archivos, nombres de archivos y directorios que se omitirán del cifrado, ejecuta comandos para evitar la recuperación de datos y finalizar una serie de procesos que potencialmente podrían interferir con el proceso.

"Este grupo emerge como un nuevo actor de amenazas que comienza con un conjunto de herramientas maduro y parece ansioso por mostrar sus capacidades, pero enfrenta la tarea de demostrar su competencia antes de poder atraer afiliados de alto calibre.

Remediación / Referencias

Por mayor información acceder a:

https://www.bitdefender.com/blog/businessinsights/hive-ransomwares-offspring-hunters-international-takes-the-stage

https://thehackernews.com/2023/11/new-ransomware-group-emerges-with-hives.html

Conclusiones

En conclusión, el panorama de la ciberseguridad sigue desafiante con el aumento alarmante de grupos de ransomware que buscan explotar vulnerabilidades en sistemas y redes. Sin embargo, ante esta amenaza en constante evolución, es esencial que la sociedad y las empresas adopten medidas proactivas para protegerse.

La concienciación y la capacitación se revelan como pilares fundamentales en la defensa contra estos ataques. La implementación de mejores prácticas, como la actualización regular de software, la adopción de medidas de seguridad avanzadas y la promoción de una cultura de ciberseguridad en todos los niveles, se destacan como estrategias clave para mitigar riesgos y fortalecer la resiliencia ante posibles amenazas.

En un mundo digital cada vez más interconectado, la colaboración y el compromiso continuo con la seguridad cibernética son esenciales para salvaguardar nuestros datos y garantizar un entorno digital más seguro y protegido para todos.

Desde el equipo de Datasec seguimos protegiendo la seguridad de nuestros clientes, socios y colaboradores.

¡Hasta la próxima!