Boletín de Ciberseguridad N°71

Fecha de publicación: 29/11/2023

Mes de noviembre

13/11/2023 – 29/11/2023

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

Aquellas noticias a tener especial recaudo son las siguientes:

Reptar: la nueva vulnerabilidad de la CPU Intel

Intel ha publicado correcciones para solucionar una falla de alta gravedad con nombre en código Reptar que afecta a sus CPU de escritorio, móviles y de servidor.

LockBit Ransomware aprovecha la vulnerabilidad crítica de Citrix

Múltiples actores de amenazas, incluidos los afiliados de ransomware LockBit, están explotando activamente una falla de seguridad crítica recientemente revelada en el control de entrega de aplicaciones (ADC) Citrix NetScaler y los dispositivos Gateway para obtener acceso inicial a los entornos de destino.

Botnet aprovecha errores de día cero en enrutadores y NVR para ataques DDoS masivos

Botnet basada en Mirai aprovecha errores de día cero en enrutadores y NVR para ataques DDoS masivos.

Vulnerabilidad Crítica

Botnet aprovecha errores de día cero en enrutadores y NVR para ataques DDoS masivos

CRÍTICO

Descripción

Botnet basada en Mirai aprovecha errores de día cero en enrutadores y NVR para ataques DDoS masivos.

Estado

Una campaña activa de malware está aprovechando dos vulnerabilidades de día cero con funcionalidad de ejecución remota de código (RCE) para conectar enrutadores y grabadores de video a una botnet de denegación de servicio distribuida (DDoS) basada en Mirai.

La carga útil se dirige a enrutadores y dispositivos de grabación de vídeo en red (NVR) con credenciales de administrador predeterminadas e instala variantes de Mirai cuando tiene éxito.

Los detalles de las fallas se encuentran actualmente en secreto para permitir a los proveedores publicar parches y evitar que otros actores de amenazas abusen de ellos. Se espera que las correcciones para una de las vulnerabilidades se envíen el próximo mes.

Los ataques fueron descubiertos por primera vez por la empresa de seguridad e infraestructura web contra sus honeypots a finales de octubre de 2023. Los autores de los ataques aún no han sido identificados.

La botnet, cuyo nombre en código es InfectedSlurs debido al uso de lenguaje racial y ofensivo en los servidores de comando y control (C2) y cadenas codificadas, es una variante del malware JenX Mirai que salió a la luz en enero de 2018.

También se identificaron muestras de malware adicionales que parecían estar relacionadas con la variante hailBot Mirai, la última de las cuales surgió en septiembre de 2023, según un análisis reciente por investigadores de seguridad.

“El hailBot se desarrolla basándose en el código fuente de Mirai, y su nombre se deriva de la cadena de información 'hail china continental' que sale después de ejecutarse”, señalaron los investigadores, detallando su capacidad de propagarse a través de la explotación de vulnerabilidades y contraseñas débiles.

El desarrollo se produce cuando al detallarse un shell web llamado wso-ng, una "iteración avanzada" de WSO (abreviatura de "web shell by oRb") que se integra con herramientas legítimas como VirusTotal y SecurityTrails mientras oculta sigilosamente su interfaz de inicio de sesión detrás de un error 404 al intentar acceder a ella.

Una de las capacidades de reconocimiento notables del web shell implica la recuperación de metadatos de AWS para su posterior movimiento lateral, así como la búsqueda de

posibles conexiones de bases de datos de Redis para obtener acceso no autorizado a datos confidenciales de las aplicaciones.

"Los shells web permiten a los atacantes ejecutar comandos en servidores para robar datos o utilizar el servidor como plataforma de lanzamiento para otras actividades como robo de credenciales, movimiento lateral, despliegue de cargas útiles adicionales o actividad práctica con el teclado, al tiempo que permiten a los atacantes persistir en una organización afectada", informó Microsoft en 2021.

El uso de web shells disponibles en el mercado también se considera un intento por parte de los actores de amenazas de desafiar los esfuerzos de atribución y pasar desapercibidos, un sello clave de los grupos de ciberespionaje que se especializan en la recopilación de inteligencia.

Remediación / Referencias

Más información en:

https://thehackernews.com/2023/11/mirai-based-botnet-exploiting-zero-day.html

https://www.akamai.com/blog/security-research/new-rce-botnet-spreads-mirai-via-zero-days

LOCKBIT 3.0	LockBit Ransomware aprovecha la vulnerabilidad crítica de Citrix	CRÍTICO

Descripción

Múltiples actores de amenazas, incluidos los afiliados de ransomware LockBit, están explotando activamente una falla de seguridad crítica recientemente revelada en el control de entrega de aplicaciones (ADC) Citrix NetScaler y los dispositivos Gateway para obtener acceso inicial a los entornos de destino.

Estado

El aviso conjunto proviene de la Agencia de Seguridad de Infraestructura y Ciberseguridad de EE. UU. (CISA), la Oficina Federal de Investigaciones (FBI), el Centro de Análisis e Intercambio de Información Multiestatal (MS-ISAC) y el Centro Australiano de Seguridad Cibernética de la Dirección Australiana de Señales (ACSC de ASD).

"Citrix Bleed, conocido por ser aprovechado por los afiliados de LockBit 3.0, permite a los actores de amenazas eludir los requisitos de contraseña y la autenticación multifactor (MFA), lo que lleva al secuestro exitoso de sesiones de usuarios legítimos en el control de entrega de aplicaciones web (ADC) de Citrix NetScaler y en los dispositivos Gateway", informaron las agencias.

"Al tomar el control de sesiones de usuarios legítimos, los actores maliciosos adquieren permisos elevados para recopilar credenciales, moverse lateralmente y acceder a datos y recursos".

Registrada con una puntuación CVSS de 9.4, Citrix abordó la vulnerabilidad el mes pasado, pero no antes de convertirla en un arma de día cero al menos desde agosto de 2023. Tiene el nombre en código Citrix Bleed.

Poco después de la divulgación pública, Mandiant, propiedad de Google, reveló que está rastreando cuatro grupos diferentes sin categoría (UNC) involucrados en la explotación de la vulnerabilidad para apuntar a varios sectores verticales de la industria en América, EMEA y APJ.

El último actor de amenazas en unirse al tren de la explotación es LockBit, que se ha observado aprovechando la falla para ejecutar scripts de PowerShell, así como eliminar herramientas de administración y monitoreo remotos (RMM) como AnyDesk y Splashtop para actividades de seguimiento.

El desarrollo subraya una vez más el hecho de que las vulnerabilidades en los servicios expuestos siguen siendo el principal vector de entrada para los ataques de ransomware.

La divulgación se produce cuando investigadores publicaron un estudio comparativo de ataques de ransomware dirigidos a Windows y Linux, señalando que la mayoría de las familias que irrumpen en Linux utilizan en gran medida la biblioteca OpenSSL junto con los algoritmos ChaCha20/RSA y AES/RSA.

"El ransomware Linux está claramente dirigido a organizaciones medianas y grandes en comparación con las amenazas de Windows, que son de naturaleza mucho más general".

El exámen de varias familias de ransomware dirigidas a Linux "revela una tendencia interesante hacia la simplificación, donde sus funcionalidades principales a menudo se reducen a procesos de cifrado básicos, dejando así el resto del trabajo a scripts y herramientas legítimas del sistema".

El equipo investigador informó que el enfoque minimalista no solo hace que estas familias de ransomware dependan en gran medida de configuraciones y scripts externos, sino que también hace que sea más fácil pasar desapercibidos.

Remediación / Referencias

Por mayor información acceder a:

https://thehackernews.com/2023/11/lockbit-ransomware-exploiting-critical.html

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-4966

Malware utiliza compresión ZPAQ en ataques de correo electrónico

CRÍTICO

Descripción

Nueva variante de malware del agente Tesla que utiliza compresión ZPAQ en ataques de correo electrónico.

Estado

Se ha observado que una nueva variante del malware Agent Tesla se entrega a través de un archivo señuelo con el formato de compresión ZPAQ para recopilar datos de varios clientes de correo electrónico y casi 40 navegadores web.

ZPAQ es un formato de compresión de archivos que ofrece una mejor relación de compresión y función de registro en diario en comparación con formatos ampliamente utilizados como ZIP y RAR.

Eso significa que los archivos ZPAQ pueden ser más pequeños, lo que ahorra espacio de almacenamiento y ancho de banda al transferir archivos. Sin embargo, ZPAQ tiene la mayor desventaja: soporte de software limitado.

Agent Tesla, que apareció por primera vez en 2014, es un registrador de teclas y un troyano de acceso remoto (RAT) escrito en .NET que se ofrece a otros actores de amenazas como parte de un modelo de malware como servicio (MaaS).

A menudo se utiliza como carga útil de primera etapa, brinda acceso remoto a un sistema comprometido y se utiliza para descargar herramientas de segunda etapa más sofisticadas, como ransomware.

El agente Tesla generalmente se entrega a través de correos electrónicos de phishing, y campañas recientes aprovechan una vulnerabilidad de corrupción de memoria de hace seis años en el Editor de ecuaciones de Microsoft Office.

La última cadena de ataques comienza con un correo electrónico que contiene un archivo adjunto ZPAQ que pretende ser un documento PDF, al abrirse se extrae un ejecutable .NET inflado que en su mayor parte está relleno con cero bytes para inflar artificialmente el tamaño de la muestra a 1 GB en un esfuerzo por evitar los métodos tradicionales.

La función principal del ejecutable .NET desarchivado es descargar un archivo con extensión .wav y descifrarlo. El uso de extensiones de archivos de uso común disfraza el tráfico como normal, lo que dificulta que las soluciones de seguridad de red detecten y prevengan actividades maliciosas.

El objetivo final del ataque es infectar el punto final con el Agente Tesla, que está ofuscado con .NET Reactor, un software de protección de código legítimo. Las comunicaciones de comando y control (C2) se realizan a través de Telegram.

El desarrollo es una señal de que los actores de amenazas están experimentando con formatos de archivos poco comunes para la entrega de malware, lo que requiere que los usuarios estén atentos a los correos electrónicos sospechosos y mantengan sus sistemas actualizados.

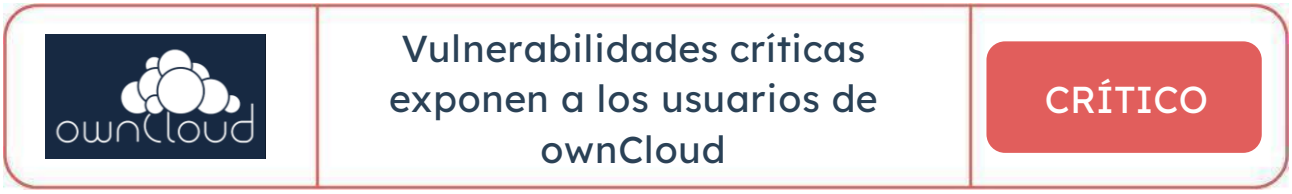
El uso del formato de compresión ZPAQ plantea más preguntas que respuestas. Las suposiciones aquí son que los actores de amenazas se dirigen a un grupo específico de personas que tienen conocimientos técnicos o utilizan herramientas de archivo menos conocidas, o están probando otras técnicas para propagar malware más rápido y evitar el software de seguridad.

Remediación / Referencias

Si deseas saber más:

https://thehackernews.com/2023/11/new-agent-tesla-malware-variant-using.html

https://cve.mitre.org/cgi-bin/cvename.cgi?name=cve-2017-11882



Descripción

Advertencia: tres vulnerabilidades críticas exponen a los usuarios de ownCloud a violaciones de datos.

Estado

Los responsables del software de intercambio de archivos de código abierto ownCloud han advertido sobre tres fallas de seguridad críticas que podrían explotarse para revelar información confidencial y modificar archivos.

Una breve descripción de las vulnerabilidades:

- Divulgación de credenciales y configuraciones confidenciales en implementaciones en contenedores que afectan las versiones de Graphapi de 0.2.0 a 0.3.0. (Puntuación CVSS: 10,0)
- Omisión de autenticación de WebDAV Api mediante URL prefirmadas que afectan las versiones principales de 10.6.0 a 10.13.0 (puntuación CVSS: 9,8)
- Omisión de validación de subdominio que afecta a oauth2 antes de la versión 0.6.1 (puntuación CVSS: 9,0)

"La aplicación 'graphapi' se basa en una biblioteca de terceros que proporciona una URL. Cuando se accede a esta URL, se revelan los detalles de configuración del entorno PHP (phpinfo)", dijo la compañía sobre la primera falla.

"Esta información incluye todas las variables de entorno del servidor web. En implementaciones en contenedores, estas variables de entorno pueden incluir datos confidenciales como la contraseña de administrador de ownCloud, las credenciales del servidor de correo y la clave de licencia".

Como solución, ownCloud recomienda eliminar el archivo "owncloud/apps/graphapi/vendor/microsoft/microsoft-graph/tests/GetPhpInfo.php" y desactivar la función 'phpinfo'. También recomienda a los usuarios que cambien secretos como la contraseña de administrador de ownCloud, las credenciales del servidor de correo y de la base de datos, y las claves de acceso a Object-Store/S3.

El segundo problema hace posible acceder, modificar o eliminar cualquier archivo sin autenticación si se conoce el nombre de usuario de la víctima y la víctima no tiene una clave de firma configurada, que es el comportamiento predeterminado.

Por último, la tercera falla se relaciona con un caso de control de acceso inadecuado que permite a un atacante "pasar una URL de redireccionamiento especialmente diseñada que omite el código de validación y, por lo tanto, le permite al atacante redirigir las devoluciones de llamada a un TLD controlado por el atacante".

Además de agregar medidas de refuerzo al código de validación en la aplicación oauth2, ownCloud ha sugerido que los usuarios deshabiliten la opción "Permitir subdominios" como solución alternativa.

La divulgación se produce cuando se lanzó un exploit de prueba de concepto (PoC) para una vulnerabilidad crítica de ejecución remota de código en la solución CrushFTP, que podría ser utilizada como arma por un atacante no autenticado para acceder a archivos y ejecutar programas arbitrarios en el host y adquirir contraseñas en texto plano.

El problema, descubierto e informado por investigadores de seguridad independientes, se soluciona en la versión 10.5.2 de CrushFTP, que se lanzó el 10 de agosto de 2023.

"Esta vulnerabilidad es crítica porque NO requiere ninguna autenticación", señaló CrushFTP en un aviso publicado en ese momento. "Se puede hacer de forma anónima y robar la sesión de otros usuarios y escalar a un usuario administrador".

Remediación / Referencias

Por mayor información acceder a:

https://thehackernews.com/2023/11/warning-3-critical-vulnerabilities.html

Grupo Kinsing aprovecha vulnerabilidad de Apache ActiveMQ

CRÍTICO

Descripción

Los piratas informáticos de Kinsing aprovechan la vulnerabilidad de Apache ActiveMQ para implementar rootkits de Linux.

Estado

Los actores de amenazas de Kinsing están explotando activamente una falla de seguridad crítica en servidores Apache ActiveMQ vulnerables para infectar sistemas Linux con rootkits y mineros de criptomonedas.

"Una vez que Kinsing infecta un sistema, implementa un script de minería de criptomonedas que explota los recursos del host para extraer criptomonedas como Bitcoin, lo que resulta en un daño significativo a la infraestructura y un impacto negativo en el rendimiento del sistema", informaron investigadores.

Kinsing se refiere a un malware de Linux con un historial de atacar entornos en contenedores mal configurados para la minería de criptomonedas, utilizando a menudo recursos del servidor comprometidos para generar ganancias ilícitas para los actores de la amenaza.

También se sabe que el grupo adapta rápidamente sus tácticas para incluir fallas recientemente reveladas en aplicaciones web para violar las redes objetivo y entregar criptomineros. A principios de este mes, se revelaron los intentos del actor de amenazas de explotar una falla de escalada de privilegios de Linux llamada Looney Tunables para infiltrarse en entornos de nube.

La última campaña implica el abuso con una puntuación CVSS de 10.0, una vulnerabilidad crítica explotada activamente en Apache ActiveMQ que permite la ejecución remota de código, lo que permite al adversario descargar e instalar el malware Kinsing.

A esto le sigue la recuperación de cargas útiles adicionales de un dominio controlado por el actor y, al mismo tiempo, se toman medidas para eliminar a los mineros de criptomonedas competidores que ya se ejecutan en el sistema infectado.

Kinsing duplica su persistencia y compromiso al cargar su rootkit en /etc/ld.so.preload, lo que completa un compromiso completo del sistema.

A la luz de la continua explotación de la falla, se recomienda a las organizaciones que ejecutan versiones afectadas de Apache ActiveMQ que actualicen a una versión parcheada lo antes posible para mitigar posibles amenazas.

La divulgación se produce cuando el Centro de respuesta a emergencias de seguridad (ASEC) de AhnLab advierte sobre ataques cibernéticos dirigidos a servidores web Apache

vulnerables para una campaña de criptojacking que aprovecha Cobalt Strike o Gh0st RAT para entregar un minero de criptomonedas.

Remediación / Referencias

Por mayor información acceder a:

https://thehackernews.com/2023/11/kinsing-hackers-exploit-apache-activemq.html

Reptar: La nueva vulnerabilidad de la CPU Intel

CRÍTICO

Descripción

Intel ha publicado correcciones para solucionar una falla de alta gravedad con nombre en código Reptar que afecta a sus CPU de escritorio, móviles y de servidor.

Estado

Registrado con una puntuación CVSS de 8.8, el problema tiene el potencial de "permitir una escalada de privilegios y/o divulgación de información y/o denegación de servicio a través del acceso local".

La explotación exitosa de la vulnerabilidad también podría permitir eludir los límites de seguridad de la CPU, según Google Cloud, que lo describió como un problema derivado de cómo el procesador interpreta los prefijos redundantes.

"El impacto de esta vulnerabilidad se demuestra cuando la explota un atacante en un entorno virtualizado multi inquilino, ya que el exploit en una máquina invitada provoca que la máquina host falle, lo que provoca una denegación de servicio a otras máquinas invitadas que se ejecutan en el mismo host", informaron desde Google Cloud.

"Además, la vulnerabilidad podría conducir potencialmente a la divulgación de información o a una escalada de privilegios".

Investigadores de seguridad, en un análisis separado de Reptar, dijeron que se puede abusar de él para corromper el estado del sistema y forzar una excepción de verificación automática.

Intel, como parte de las actualizaciones de noviembre de 2023, ha publicado un microcódigo actualizado para todos los procesadores afectados. La lista completa de CPU Intel afectadas no se encuentra disponible. No hay evidencia de ningún ataque activo que utilice esta vulnerabilidad.

"Intel no espera que este problema sea encontrado por ningún software no malicioso del mundo real", dijo la compañía en una guía publicada el 14 de noviembre. "La explotación maliciosa de este problema requiere la ejecución de código arbitrario".

La divulgación coincide con el lanzamiento de parches para una falla de seguridad en los procesadores AMD llamada CacheWarp, que permite a actores maliciosos ingresar a máquinas virtuales protegidas por AMD SEV para escalar privilegios y obtener ejecución remota de código.

Remediación / Referencias

Por mayor información acceder a:

https://thehackernews.com/2023/11/zero-day-alert-lace-tempest-exploits.html

Conclusiones

En el vertiginoso paisaje digital actual, la proliferación de técnicas avanzadas de malware y phishing ha llevado la ciberseguridad a una encrucijada crítica.
La interconexión global, si bien ha traído consigo innumerables beneficios, también ha abierto la puerta a amenazas más sofisticadas y omnipresentes que nunca. Este boletín ha arrojado luz sobre la creciente complejidad de estos ataques, destacando la necesidad urgente de una postura proactiva y educativa para salvaguardar nuestras redes y datos.

La rapidez con la que evolucionan las tácticas de malware y phishing exige una respuesta igualmente ágil por parte de individuos, empresas y gobiernos. La prevención se convierte en el pilar fundamental en esta batalla digital, y la educación emerge como el arma más poderosa. Capacitar a los usuarios para reconocer las señales de amenazas potenciales, inculcar prácticas seguras en el uso de la tecnología y promover la conciencia constante son elementos esenciales para construir un frente unido contra los ciberataques.

En este sentido, la colaboración entre sectores se vuelve imperativa. Empresas, organismos gubernamentales, y la sociedad en su conjunto deben unir fuerzas para compartir información, adoptar las mejores prácticas y fortalecer las defensas colectivas.
La ciberseguridad ya no es un desafío aislado, sino un esfuerzo conjunto para preservar la integridad de nuestra infraestructura digital.

En conclusión, el escenario actual exige una respuesta integral y adaptable. Al centrarnos en la prevención y la educación, podemos erigir barreras digitales más robustas, desafiando las tácticas en constante evolución de los actores malintencionados. La resiliencia frente a las amenazas cibernéticas comienza con el conocimiento y la acción consciente. Al abrazar este enfoque, estamos construyendo un futuro digital más seguro y resistente para todos.

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

¡Hasta la próxima!