Boletín de Ciberseguridad

Fecha de Publicación
06/12/2021 - N.º 22

Mes de diciembre
22/11/2021 - 06/12/2021

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 las 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 primera quincena del mes de diciembre se destacan 6 noticias de relevancia: 2 sobre vulnerabilidades tecnológicas, 3 de fraudes activos y 1 de prevención.

Aquellas noticias a tener especial recaudo son las siguientes:

Zero-Day: elevación de privilegios en Windows

Zero Day que afecta a Windows 10, Windows 11 y Windows Server permite que cualquiera obtenga derechos de administrador.

1.2 millones de usuarios de Wordpress afectados por brecha de datos de GoDaddy

Una brecha de seguridad expuso las direcciones de correo electrónico y los números de clientes de más de 1.2 millones de usuarios de WordPress de la empresa de alojamiento web GoDaddy.

Actores maliciosos hackearon plataformas de Google Cloud para minar criptomonedas

El informe del Equipo de Acción de Ciberseguridad de Google descubrió que los piratas informáticos estaban realizando minería de criptomonedas, una actividad intensiva en recursos de la nube y con fines de lucro, dentro de las instancias comprometidas de las cuentas de Google Cloud.

ZERO-DAY	**Zero-Day: elevación de privilegios en Windows**	CRÍTICO

Descripción

Zero Day que afecta a Windows 10, Windows 11 y Windows Server permite que cualquiera obtenga derechos de administrador.

Estado

Este mes se reveló que una vulnerabilidad de Microsoft que permite la elevación local de privilegios, previamente parcheada en el martes de parche de noviembre de 2021, sigue siendo explotable y no fue parcheada correctamente.

Aprovechando este fallo, los actores de la amenaza con acceso a una cuenta de usuario estándar limitada en una instalación vulnerable de Windows pueden elevar fácilmente los privilegios del usuario, y luego moverse lateralmente dentro de la red para llevar a cabo múltiples actividades maliciosas.

El experto en seguridad que reveló originalmente la vulnerabilidad posteriormente corregida, encontró un bypass que conducía a la nueva y más potente vulnerabilidad de elevación de privilegios.

Por lo que lanzó un exploit de prueba de concepto (PoC) denominado "InstallerFileTakeOver" completamente funcional para la nueva vulnerabilidad de día cero de Windows Installer. El PoC permite a los piratas informáticos obtener privilegios de administrador cuando inician sesión en una máquina Windows con Edge instalado.

Como resultado, un adversario puede ejecutar cualquier código malicioso como administrador. En particular, InstallerFileTakeOver permite omitir las políticas de grupo que impiden que los usuarios "estándar" inicien operaciones de instalación de MSI, lo que hace que el exploit PoC sea aún más peligroso.

Remediación / Referencias

Al no haber un parche oficial en este momento, recomendamos se preparen para parchear esto tan pronto como se publique la solución oficial.

Por mayor información acceder a:
https://blog.segu-info.com.ar/2021/11/zero-day-que-permite-elevacion-de.html

Printing Shellz: fallos afectan a 150 modelos de impresoras multifunción de HP

CRÍTICO

Descripción

Investigadores de seguridad han descubierto dos vulnerabilidades en las impresoras multifunción de HP que afectaron a 150 modelos de productos.
Se remontan a 2013 y podrían haber expuesto a sus usuarios a ciberataques desde entonces.

Estado

Expertos utilizaron una impresora multifunción (MFP) HP M725z como entorno de prueba para comprobar su firmware en busca de vulnerabilidades. Encontraron varias fallas en el firmware de al menos 150 impresoras multifunción (impresión, escaneo, fax) del fabricante Hewlett Packard.

Los dispositivos HP contienen los siguientes fallos en su firmware:

- La primera corresponde a Divulgación de información con un CVSS 7.1 (Alto) y es un fallo de divulgación de información causado por un puerto físico expuesto; es necesario el acceso local como vector de ataque.

- El segundo fallo corresponde a Potencial desbordamiento de búfer con CVSS 9.3 (Crítico).
  El desbordamiento de búfer en el analizador de fuentes del firmware se considera crítico debido al temor a la ejecución remota de código (RCE). Además, la vulnerabilidad se clasifica como "desparasitable", lo que significa que un atacante podría distribuir su malware a toda una red corporativa a través de una impresora infectada.

Los actores de la amenaza pueden explotar ambas fallas localmente a través del acceso físico al dispositivo vulnerable, por ejemplo, imprimiendo a través de USB, imprimiendo por correo electrónico o invocando la impresión a través de un navegador con código JavaScript en una página web.

El informe afirmó que también podría permitir a los atacantes lanzar ataques más profundos en la red corporativa para difundir ransomware, robar datos de almacenes de datos más confidenciales y lograr otros objetivos.

Remediación / Referencias

Se recomienda instalar la actualización de firmware disponible para el dispositivo específico ya que la divulgación pública de las vulnerabilidades probablemente desencadenará una oleada de ataques que intentarán aprovecharse de ellas.

Si desea saber más al respecto:
https://unaaldia.hispasec.com/2021/12/vulnerabilidades-criticas-en-impresoras-hp.html

GoDaddy	**1.2 millones de usuarios de Wordpress afectados por brecha de datos de GoDaddy**	CRÍTICO

Descripción

Una brecha de seguridad expuso las direcciones de correo electrónico y los números de clientes de más de 1.2 millones de usuarios de WordPress de la empresa de alojamiento web GoDaddy.

Afectados

Los afectados fueron 1.2 millones de usuarios tanto activos como inactivos de Wordpress.

Estado

GoDaddy reveló la infracción y confirmó que a millones de usuarios de su servicio de alojamiento administrado de WordPress se les robaron datos confidenciales.

La violación de datos aparentemente fue descubierta por Wordfence, un complemento de terceros que es popular entre los usuarios de Wordpress para la seguridad básica automatizada de sitios web.

El ataque habría comenzado el 6 de setiembre, pero no fue hasta el 17 de noviembre que la empresa de alojamiento descubrió que un intruso había obtenido acceso a su entorno de alojamiento administrado de WordPress.

El acceso no autorizado de terceros se llevó a cabo por medio del sistema de aprovisionamiento en la base de código heredado para usuarios de Wordpress con cuentas administradas.

Los datos comprometidos fueron:

- Dirección de correo electrónico y número de cliente de 1.2 millones de usuarios activos e inactivos de Wordpress.
- Contraseña de administrador de WordPress original que se estableció en el momento del aprovisionamiento.
- Para los clientes activos, nombres de usuario y contraseñas de sFTP y bases de datos.
- Para un subconjunto de clientes activos, la clave privada SSL.

Remediación / Referencias

Todas las contraseñas afectadas fueron reestablecidas y GoDaddy está en proceso de emitir e implementar nuevos certificados para los clientes cuyas claves SSL estaban expuestas.

Por mayor información al respecto se puede acceder a:
https://blog.segu-info.com.ar/2021/11/brecha-en-godaddy-expone-datos-de-12.html

	**Actores maliciosos hackearon plataformas de Google Cloud para minar criptomonedas**	IMPORTANTE

Descripción

El informe del Equipo de Acción de Ciberseguridad de Google descubrió que los piratas informáticos estaban realizando minería de criptomonedas, una actividad intensiva en recursos de la nube y con fines de lucro, dentro de las instancias comprometidas de las cuentas de Google Cloud.

Estado

En un informe destinado a evaluar las amenazas a los usuarios de la nube, el Equipo de Acción de Ciberseguridad de Google dijo que algunos atacantes están explotando cuentas "mal configuradas" para extraer criptomonedas.

De 50 incidentes analizados que comprometieron el Protocolo de Google Cloud, el 86% estaban relacionados con la minería de criptomonedas.

Alrededor del 10% de las cuentas comprometidas también se utilizaron para realizar escaneos de otros recursos disponibles públicamente en Internet para identificar sistemas vulnerables, mientras que el 8% de las instancias se utilizaron para atacar otros objetivos.

Alrededor de una cuarta parte de las cuentas comprometidas se debieron a vulnerabilidades en software de terceros que había sido instalado por el propietario.

Los expertos en ciberseguridad informaron que muchos de los ataques no se limitaron a una sola acción maliciosa como la minería de criptomonedas, sino que también fueron puntos de preparación para realizar otros ataques e identificar otros sistemas vulnerables.

Google dijo que los ciberdelincuentes pudieron acceder a las cuentas de Google Cloud aprovechando las malas prácticas de seguridad de los clientes. Casi la mitad de las cuentas comprometidas se atribuyeron a actores que obtuvieron acceso a una cuenta en la nube orientada a Internet que no tenía contraseña o tenía una contraseña débil. Como resultado, estas cuentas de Google Cloud podrían escanearse fácilmente y forzarse brutalmente.

La velocidad de los ataques también fue digna de mención. Según el análisis de Google, los piratas informáticos pudieron descargar software de minería criptográfica a las cuentas comprometidas en 22 segundos en la mayoría de los incidentes analizados. Google sugirió que *"los ataques iniciales y las descargas posteriores fueron eventos programados que no requerían intervención humana"* y dijo que sería casi imposible intervenir manualmente para detener tales incidentes una vez que comenzaran.

En otra parte del informe, Google dijo que el grupo de hackers APT28, también conocido como Fancy Bear, respaldado por el gobierno ruso, atacó 12.000 cuentas de Gmail en un intento masivo de phishing, en el que se engaña a los usuarios para que entreguen sus datos de acceso. Los atacantes intentaron engañar a los titulares de las cuentas para que entregaran sus datos a través de un correo electrónico que decía: "Creemos que atacantes respaldados por el gobierno pueden estar intentando engañarle para conseguir la contraseña de su cuenta". Google dijo que había bloqueado todos los correos electrónicos de phishing en el ataque -que se centró en el Reino Unido, los Estados Unidos y la India- y que no se habían comprometido los datos de los usuarios.

Remediación / Referencias

Para prevenir tales ataques, Google recomendó varios enfoques de seguridad diferentes, incluido el análisis en busca de vulnerabilidades, el uso de autenticación de dos factores y la implementación del producto Work Safer de Google para la seguridad.

Entérate demás:
https://services.google.com/fh/files/misc/gcat_threathorizons_full_nov2021.pdf
https://blog.segu-info.com.ar/2021/11/aprovechan-google-cloud-para-minar.html

JS	Nuevo malware de JavaScript funciona como un dispensador de RAT	IMPORTANTE

Descripción

Expertos en ciberseguridad descubrieron una nueva cepa de malware JavaScript que los ciberdelincuentes están utilizando como una forma de infectar sistemas y luego implementar peligrosos troyanos de acceso remoto (RAT).

Estado

Inteligentemente llamado RATDispenser, el malware se ha distribuido de forma salvaje durante al menos tres meses en forma de mensajes de correo electrónico con archivos adjuntos maliciosos.

RATDispenser llega como un archivo adjunto malicioso en un correo electrónico de phishing. Al igual que la mayoría de los ataques con malware JavaScript, RATDispenser se utiliza para ganar un punto de apoyo inicial en un sistema antes de lanzar malware secundario que establece el control sobre el dispositivo comprometido.

El cargador del programa malicioso se distribuye a través de correo electrónico no deseado como un archivo adjunto New Order.TXT .js.
Si el usuario hace doble clic, se ejecutará, momento en el que el JavaScript ofuscado se decodifica a sí mismo y escribe un archivo VBScript en una carpeta temporal usando cmd.exe.
Este archivo VBScript luego descarga la carga útil del malware y, si tiene éxito, se eliminará a sí mismo posteriormente.

Estos archivos abusan del truco clásico de doble extensión (nombre de archivo.txt.js) para hacerse pasar por archivos de texto, pero ejecutan código JavaScript cuando los usuarios intentan abrirlos.
Los investigadores escriben que el RATDispenser parece eludir efectivamente los controles de seguridad con una tasa de detección del 11% y han identificado ocho familias de malware en 2021 que se distribuyen a través del RATDispenser.

Todas las muestras de malware cargadas eran troyanos de acceso remoto (RAT) diseñados para robar información y dar a los atacantes control sobre los dispositivos de las víctimas.

Remediación/ Referencias

Bloquear archivos JS/VBS/RTF en el correo entrante de tu organización.

Puedes acceder a toda la información en el siguiente link:
https://threatresearch.ext.hp.com/javascript-malware-dispensing-rats-into-the-wild/#

	Vulnerabilidad de ejecución remota de código de Microsoft Exchange Server	PREVENCIÓN

Descripción

El código de explotación de prueba de concepto se lanzó en línea para una vulnerabilidad de alta gravedad explotada activamente que afecta a los servidores de Microsoft Exchange.

Afectados

El fallo de seguridad afecta a Exchange Server 2016 y Exchange Server 2019 locales.

Estado

La falla es un problema de ejecución remota de código de alta gravedad que se produce debido a una validación incorrecta de los argumentos del cmdlet y solo puede ser explotada por un atacante autenticado.

Microsoft abordó la falla con el lanzamiento de las actualizaciones de seguridad del martes de parches de Microsoft para noviembre de 2021. Luego de esta publicación del parche, un investigador publicó un exploit de prueba de concepto para el error de RCE posterior a la autenticación de Exchange.

Remediación / Referencias

Los administradores deben instalar inmediatamente los parches publicados en el martes de parches de noviembre de Microsoft y aquellos que utilizan servidores Exchange también deberían comprobar si los atacantes han intentado aprovecharse de ellos.

Por mayor información al respecto se puede acceder a:
https://www.bleepingcomputer.com/news/security/exploit-released-for-microsoft-exchange-rce-bug-patch-now/

Conclusiones

Otra quincena en dónde les acercamos jugosas noticias de ciberseguridad.
En esta oportunidad vemos la importancia de los proveedores en la cadena de suministros tecnológicos, en la que observamos la relevancia de conocer dónde se encuentran nuestros datos y bajo qué circunstancias.

En el ámbito de la nube, esto implica reconocer bien cuales son los límites y responsabilidades que tiene tanto el proveedor como nuestros equipos de trabajo sobre los ambientes de activos. Por ejemplo, la noticia sobre un incidente en el proveedor de Hosting y nombres de dominio; GoDaddy, entendiendo que este incidente se originó en las cuentas que hayan adquirido el paquete de software Wordpress en la plataforma, de lo contrario no estarían siendo afectados otros tipos de cuentas.

En el caso de Google Cloud, Azure, AWS y otras plataformas de servicios tipo IaaS, observamos la importancia de mantener monitoreo y visibilidad sobre los recursos y registros, a fin de descubrir de forma temprana aspectos negativos que pudieran afectarlos, como por ejemplo los referidos a minado de criptomonedas, entre otros eventos.

Hay que recordar que estos servicios IaaS en la nube requieren que a nivel lógico sean los operadores de nuestras organizaciones los que deberán mantener las operaciones y seguridad de ese entorno, que se encuentra en general de manera pública y son fácilmente descubribles, por lo que suelen ser foco de amenazas de este estilo.

Recomendamos a las organizaciones que mantengan este tipo de infraestructuras, contar con el monitoreo adecuado y preventivo, por ejemplo a través de herramientas como SIEM que pueden estar siendo monitoreadas por un equipo de SOC que alertará y empujará para reforzar los aspectos de ciberseguridad que requieran ajustes.

Recomendamos el seguimiento y revisión de las infraestructuras en la nube a través de estos 10 puntos recomendados por OWASP: https://hitachi-systems-security.com/the-top-10-owasp-cloud-security-risks/