Boletín de Ciberseguridad N°60

Fecha de publicación: 05/06/2023

Mes de junio

23/05/2023 – 05/06/2023

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 primera quincena del mes de junio se destacan 5 noticias de relevancia: 4 sobre vulnerabilidades tecnológicas, y 1 de prevención.

Aquellas noticias a tener especial recaudo son las siguientes:

Vulnerabilidad crítica de firmware en sistemas Gigabyte

Una falla crítica en la aplicación de transferencia de archivos administrada MOVEit Transfer de Progress Software ha sido objeto de una explotación generalizada en la realidad para hacerse cargo de los sistemas vulnerables.

Microsoft detalla la vulnerabilidad crítica de Apple

Microsoft ha compartido detalles de una falla ahora parcheada en Apple macOS que podría ser abusada por actores de amenazas con acceso de raíz para eludir las medidas de seguridad y realizar acciones arbitrarias en los dispositivos afectados.

Una falla grave en el servicio Cloud SQL de Google Cloud

Se ha revelado una nueva falla de seguridad en el servicio Cloud SQL de Google Cloud Platform (GCP) que podría explotarse potencialmente para obtener acceso a datos confidenciales.

Vulnerabilidad Crítica

Progress MOVEit	**Transferencia de MOVEit bajo ataque**	CRÍTICO

Descripción

Una falla crítica en la aplicación de transferencia de archivos administrada MOVEit Transfer de Progress Software ha sido objeto de una explotación generalizada en la realidad para hacerse cargo de los sistemas vulnerables.

Estado

La deficiencia, a la que se le asigna el identificador CVE CVE-2023-34362, se relaciona con una grave vulnerabilidad de inyección de SQL que podría dar lugar a una escalada de privilegios y un posible acceso no autorizado al entorno.

La empresa con sede en Massachusetts, que también es propietaria de Telerik, ha puesto a disposición parches para el error en las siguientes versiones: 2021.0.6 (13.0.6), 2021.1.4 (13.1.4), 2022.0.4 (14.0.4), 2022.1.5 (14.1.5) y 2023.0.1 (15.0.1).

Los intentos de explotación exitosos culminan con la implementación de un shell web, un archivo llamado "human2.aspx" en el directorio "wwwroot" que se crea a través de un script con un nombre de archivo aleatorio, para "exfiltrar varios datos almacenados por el servicio MOVEit local".

El shell web también está diseñado para agregar nuevas sesiones de cuenta de usuario administrador con el nombre "Servicio de verificación de estado" en un probable esfuerzo por eludir la detección, según reveló un análisis de la cadena de ataque.

El desarrollo ha llevado a la Agencia de Seguridad de Infraestructura y Ciberseguridad de EE. UU. (CISA) a emitir una alerta , instando a los usuarios y organizaciones a seguir los pasos de mitigación para protegerse contra cualquier actividad maliciosa.

Remediación / Referencias

Se recomienda aislar los servidores bloqueando el tráfico entrante y saliente e inspeccionar los entornos en busca de posibles indicadores de compromiso (IoC) y, de ser así, eliminarlos antes de aplicar las correcciones.

Por mayor información acceder a:

https://www.ipswitch.com/es/moveit-transfer

GIGABYTE™	Vulnerabilidad crítica de firmware en sistemas Gigabyte	CRÍTICO

Descripción

Se ha encontrado un "comportamiento similar a una puerta trasera" dentro de los sistemas Gigabyte, que dicen que permite que el firmware UEFI de los dispositivos suelte un ejecutable de Windows y recupere actualizaciones en un formato no seguro.

Estado

La firma de seguridad de firmware Eclypsium dijo que detectó la anomalía por primera vez en abril de 2023. Desde entonces, Gigabyte reconoció y abordó el problema.

El ejecutable, según Eclypsium, está integrado en el firmware UEFI y el firmware lo escribe en el disco como parte del proceso de arranque del sistema y, posteriormente, se inicia como un servicio de actualización.

La aplicación basada en .NET, por su parte, está configurada para descargar y ejecutar una carga útil desde los servidores de actualización de Gigabyte a través de HTTP simple, lo que expone el proceso a ataques de adversario en el medio (AitM) a través de un enrutador comprometido.

Loucaides dijo que el software "parece haber sido pensado como una aplicación de actualización legítima ", y señaló que el problema podría afectar "alrededor de 364 sistemas Gigabyte con una estimación aproximada de 7 millones de dispositivos".

Remediación / Referencias

Se recomienda que se apliquen las últimas actualizaciones de firmware para minimizar los riesgos potenciales. También se recomienda inspeccionar y deshabilitar la función "Descarga e instalación del centro de aplicaciones" en la configuración de UEFI/BIOS y establecer una contraseña de BIOS para evitar cambios maliciosos.

Por mayor información acceder a:

https://vulners.com/thn/THN:0F0CFDDD881C0942F795101A3DBBB9DF

	Microsoft detalla la vulnerabilidad crítica de Apple	CRÍTICO

Descripción

Microsoft ha compartido detalles de una falla ahora parcheada en Apple macOS que podría ser abusada por actores de amenazas con acceso de raíz para eludir las medidas de seguridad y realizar acciones arbitrarias en los dispositivos afectados.

Estado

Específicamente, la falla, denominada Migraña y rastreada como CVE-2023-32369, podría abusarse para eludir una medida de seguridad clave llamada Protección de integridad del sistema (SIP), o "sin raíz", que limita las acciones que el usuario raíz puede realizar en protegidos. archivos y carpetas.

La omisión es posible gracias a una herramienta integrada de macOS llamada Asistente de migración para activar el proceso de migración a través de un AppleScript que está diseñado para, en última instancia, lanzar una carga útil arbitraria.

Esto, a su vez, se debe al hecho de que systemmigrationd, el daemon utilizado para manejar la transferencia de dispositivos, viene con el derecho com.apple.rootless.install.heritable, lo que permite que todos sus procesos secundarios, incluidos bash y perl, omitan las comprobaciones SIP.

Tras la divulgación responsable, Apple abordó la vulnerabilidad como parte de las actualizaciones (macOS Ventura 13.4, macOS Monterey 12.6.6 y macOS Big Sur 11.7.7) enviadas el 18 de mayo de 2023.

El fabricante de iPhone describió CVE-2023-32369 como un problema de lógica que podría permitir que una aplicación maliciosa modifique partes protegidas del sistema de archivos.

Remediación / Referencias

Se recomienda a los usuarios que realicen las últimas actualizaciones en sus dispositivos.

Por mayor información acceder a:

https://www.microsoft.com/en-us/security/blog/2023/05/30/new-macos-vulnerability-migraine-could-bypass-system-integrity-protection/

	Una falla grave en el servicio Cloud SQL de Google Cloud	CRÍTICO

Descripción

Se ha revelado una nueva falla de seguridad en el servicio Cloud SQL de Google Cloud Platform (GCP) que podría explotarse potencialmente para obtener acceso a datos confidenciales.

Estado

La cadena de ataque de múltiples etapas identificados, aprovechó una brecha en la capa de seguridad de la plataforma en la nube asociada con SQL Server para escalar los privilegios de un usuario a un rol de administrador.

Posteriormente, los permisos elevados permitieron abusar de otra configuración errónea crítica para obtener derechos de administrador del sistema y tomar el control total del servidor de la base de datos.

A partir de ahí, un actor de amenazas podría acceder a todos los archivos alojados en el sistema operativo subyacente, enumerar archivos y extraer contraseñas, que luego podrían actuar como una plataforma de lanzamiento para futuros ataques.

Remediación / Referencias

Luego de la divulgación responsable en febrero de 2023, Google abordó el problema en abril de 2023.

Por mayor información acceder a:

https://cloud.google.com/sql/docs/troubleshooting?hl=es-419

Prevención

Actualización urgente de WordPress

PREVENCIÓN

Descripción

WordPress ha emitido una actualización automática para corregir una falla crítica en el complemento Jetpack que está instalado en más de cinco millones de sitios.

Estado

La vulnerabilidad, que se descubrió durante una auditoría de seguridad interna, reside en una API de PHP. Si bien no hay evidencia de que el problema haya sido explotado en la realidad, no es raro que las fallas en los complementos populares de WordPress sean aprovechadas por los actores de amenazas que buscan apoderarse de los sitios con fines maliciosos.

Esta no es la primera vez que las debilidades de seguridad severas en Jetpack han llevado a WordPress a forzar la instalación de los parches.

El desarrollo también se produce cuando Patchstack reveló una falla de seguridad en el complemento premium Gravity Forms que podría permitir que un usuario no autenticado inyecte código PHP arbitrario.

Remediación / Referencias

El problema (CVE-2023-28782) afecta a todas las versiones a partir de la 2.7.3 y anteriores. Se ha abordado en la versión 2.7.4, que estuvo disponible el 11 de abril de 2023.

Por mayor información acceder a:

https://cert.civis.net/en/index.php?action=alert&param=CVE-2023-28782

Conclusiones

Este boletín informativo quincenal destaca noticias relevantes en el campo de la ciberseguridad a nivel regional e internacional. Se abordan categorías como vulnerabilidades tecnológicas, fraudes activos, amenazas emergentes y recomendaciones de prevención. En la primera quincena de junio, se resaltan cinco noticias importantes: cuatro sobre vulnerabilidades tecnológicas y una sobre prevención.

Las noticias destacadas son las siguientes:

- Vulnerabilidad crítica de firmware en sistemas Gigabyte: Se descubrió una falla en los sistemas Gigabyte que permite que el firmware UEFI libere un ejecutable de Windows y recupere actualizaciones de manera insegura. Se recomienda aplicar las últimas actualizaciones de firmware y deshabilitar la función de descarga e instalación del centro de aplicaciones.
- Microsoft detalla la vulnerabilidad crítica de Apple: Microsoft compartió detalles sobre una falla en Apple macOS que podría ser abusada por actores de amenazas con acceso de raíz para eludir las medidas de seguridad. Apple ha abordado esta vulnerabilidad en las actualizaciones recientes.
- Falla grave en el servicio Cloud SQL de Google Cloud: Se reveló una nueva falla de seguridad en el servicio Cloud SQL de Google Cloud Platform que podría permitir el acceso a datos confidenciales. Google ha solucionado este problema después de una divulgación responsable.
- Actualización crítica del complemento Jetpack de WordPress: WordPress emitió una actualización automática para corregir una falla crítica en el complemento Jetpack que afectaba a más de cinco millones de sitios. Se recomienda instalar la versión actualizada para proteger los sitios.

Estas noticias resaltan la importancia de aplicar actualizaciones de firmware y software, así como de tomar medidas de seguridad adicionales para proteger los sistemas y datos.

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

¡Sigan protegiéndose!