Boletín de Ciberseguridad N°61

Fecha de publicación: 26/06/2023

Mes de junio

05/06/2023 – 26/06/2023

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 este mes de junio se destacan 5 noticias de relevancia: 2 sobre vulnerabilidades tecnológicas, y 3 de prevención.

Aquellas noticias a tener especial recaudo son las siguientes:

Se agregan 6 fallas al catálogo de vulnerabilidades explotadas

La Agencia de Seguridad de Infraestructura y Ciberseguridad de EE. UU. agregó un lote de seis fallas a su catálogo de Vulnerabilidades Explotadas Conocidas (KEV), citando evidencia de explotación activa.

Se advierte sobre troyano GravityRAT para Android

Se encontró una versión actualizada de un troyano de acceso remoto de Android denominado GravityRAT disfrazado de aplicaciones de mensajería BingeChat y Chatico como parte de una campaña específica desde junio de 2022.

ASUS lanza parches para corregir errores de seguridad

ASUS lanzó el lunes actualizaciones de firmware para abordar, entre otros problemas, nueve errores de seguridad que afectan a una amplia gama de modelos de enrutadores.

Vulnerabilidad Crítica

Se agregan 6 fallas al catálogo de vulnerabilidades explotadas

CRÍTICO

Descripción

La Agencia de Seguridad de Infraestructura y Ciberseguridad de EE. UU. agregó un lote de seis fallas a su catálogo de Vulnerabilidades Explotadas Conocidas (KEV), citando evidencia de explotación activa.

Estado

Esto comprende tres vulnerabilidades que Apple corrigió esta semana (CVE-2023-32434, CVE-2023-32435 y CVE-2023-32439), dos fallas en VMware (CVE-2023-20867 y CVE-2023-20887) y una Defecto que afecta a los dispositivos Zyxel (CVE-2023-27992).

Se dice que CVE-2023-32434 y CVE-2023-32435, que permiten la ejecución de código, se explotaron como días cero para implementar spyware como parte de una campaña de espionaje cibernético de un año de duración que comenzó en 2019.

Apodada Operación Triangulación, la actividad culmina con la implementación de TriangleDB que está diseñado para recopilar una amplia gama de información de dispositivos comprometidos, como crear, modificar, eliminar y robar archivos, enumerar y finalizar procesos, recopilar credenciales de iCloud Keychain y rastrear la ubicación de un usuario.

La cadena de ataque comienza cuando la víctima objetivo recibe un iMessage con un archivo adjunto que activa automáticamente la ejecución de la carga útil sin necesidad de interacción alguna, lo que lo convierte en un exploit sin clic.

CVE-2023-32434 y CVE-2023-32435 son dos de las muchas vulnerabilidades en iOS de las que se ha abusado en el ataque de espionaje. Uno de ellos es CVE-2022-46690 , un problema de escritura fuera de los límites de alta gravedad en IOMobileFrameBuffer que podría convertirse en un arma mediante una aplicación no autorizada para ejecutar código arbitrario con privilegios de kernel.

Remediación / Referencias

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

Por mayor información acceder a:

https://nvd.nist.gov/vuln/detail/CVE-2023-2828

Vulnerabilidades en Microsoft Azure Bastion

CRÍTICO

Descripción

Se han revelado dos vulnerabilidades de seguridad "peligrosas" en Microsoft Azure Bastion y Azure Container Registry que podrían haberse aprovechado para llevar a cabo ataques de secuencias de comandos entre sitios (XSS).

Estado

Las dos fallas identificadas por Orca aprovechan una debilidad en el iframe postMessage, que permite la comunicación de origen cruzado entre los objetos de Windows.

Esto significa que se podía abusar de la deficiencia para incrustar puntos finales dentro de servidores remotos usando la etiqueta iframe y, en última instancia, ejecutar código JavaScript malicioso, lo que pondría en peligro datos confidenciales.

Sin embargo, para explotar estas debilidades, un actor de amenazas tendría que realizar un reconocimiento en diferentes servicios de Azure para identificar los puntos finales vulnerables integrados en el portal de Azure que pueden tener encabezados de X-Frame-Options faltantes o Políticas de seguridad de contenido (CSP) débiles.

Luego de la divulgación responsable de las fallas el 13 de abril y el 3 de mayo de 2023, Microsoft implementó correcciones de seguridad para remediarlas. No se requiere ninguna otra acción por parte de los usuarios de Azure.

Remediación / Referencias

Se lanzaron una serie de correcciones para rectificar las debilidades de XSS y no se encontró evidencia de explotación activa más allá del PoC ideado por la empresa de seguridad en la nube con sede en Oregón.

Por mayor información acceder a:

https://learn.microsoft.com/en-us/security/benchmark/azure/baselines/bastion-security-baseline

Prevención

	Se advierte sobre troyano GravityRAT para Android	**PREVENCIÓN**

Descripción

Se encontró una versión actualizada de un troyano de acceso remoto de Android denominado GravityRAT disfrazado de aplicaciones de mensajería BingeChat y Chatico como parte de una campaña específica desde junio de 2022.

Estado

GravityRAT es el nombre que se le da a un malware multiplataforma que es capaz de atacar dispositivos Windows, Android y macOS. La firma de ciberseguridad eslovaca está rastreando la actividad bajo el nombre de SpaceCobra.

Se sospecha que el actor de amenazas tiene su base en Pakistán, con ataques recientes que involucran a GravityRAT contra personal militar en India y entre la Fuerza Aérea de Pakistán al camuflarlo como aplicaciones de entretenimiento y almacenamiento en la nube, como lo reveló Meta el mes pasado.

El uso de aplicaciones de chat como señuelo para distribuir el malware fue destacado previamente en noviembre de 2021 por Cyble, que analizó una muestra llamada "SoSafe Chat" que se cargó en la base de datos VirusTotal desde India.

El modus operandi sugiere que se contacta a los objetivos potenciales en Facebook e Instagram con el objetivo de engañarlos para que hagan clic en los enlaces y descarguen las aplicaciones maliciosas.

Remediación / Referencias

Se recomienda a los usuarios a tener cuidado y abstenerse de seguir canales de minería de criptomonedas sospechosos en plataformas como Telegram, ya que estos canales pueden generar pérdidas financieras sustanciales y comprometer datos personales confidenciales

Por mayor información acceder a:

https://crast.net/es/359315/whatsapp-meet-gravityrat-the-trojan-virus-behind-backup-copies/

Apple lanza parches para fallas explotadas activamente

PREVENCIÓN

Descripción

Apple lanzó una serie de actualizaciones para iOS, iPadOS, macOS, watchOS y el navegador Safari para abordar un conjunto de fallas que, según dijo, se explotaron activamente en la naturaleza.

Estado

Esto incluye un par de días cero que se han armado en una campaña de vigilancia móvil llamada Operación Triangulación que ha estado activa desde 2019. Se desconoce el actor de amenazas exacto detrás de la actividad.

- CVE-2023-32434 : una vulnerabilidad de desbordamiento de enteros en el Kernel que podría ser explotada por una aplicación maliciosa para ejecutar código arbitrario con privilegios de kernel.
- CVE-2023-32435 : una vulnerabilidad de corrupción de memoria en WebKit que podría conducir a la ejecución de código arbitrario al procesar contenido web especialmente diseñado.

El aviso se produce cuando el proveedor ruso de seguridad cibernética analizó el implante de spyware utilizado en la campaña de ataque sin clic dirigida a dispositivos iOS a través de iMessages que contenía un archivo adjunto integrado con un exploit para la vulnerabilidad de ejecución remota de código (RCE) del kernel.

Remediación / Referencias

La falla explotada activamente, descrita como un problema de confusión de tipos, se ha solucionado con controles mejorados. Las actualizaciones están disponibles para las siguientes plataformas:

- iOS 16.5.1 y iPadOS 16.5.1 : iPhone 8 y posteriores, iPad Pro (todos los modelos), iPad Air de 3.ª generación y posteriores, iPad de 5.ª generación y posteriores y iPad mini de 5.ª generación y posteriores
- iOS 15.7.7 y iPadOS 15.7.7 : iPhone 6s (todos los modelos), iPhone 7 (todos los modelos), iPhone SE (1.ª generación), iPad Air 2, iPad mini (4.ª generación) y iPod touch (7.ª generación)
- macOS Ventura 13.4.1 , macOS Monterey 12.6.7 y macOS Big Sur 11.7.8
- watchOS 9.5.2 - Apple Watch Series 4 y posteriores
- watchOS 8.8.1 : Apple Watch Series 3, Series 4, Series 5, Series 6, Series 7 y SE, y
- Safari 16.5.1 : Mac con macOS Monterey

Por mayor información acceder a:

https://nvd.nist.gov/vuln/detail/CVE-2023-32434

ASUS	**ASUS lanza parches para corregir errores de seguridad**	PREVENCIÓN

Descripción

ASUS lanzó el lunes actualizaciones de firmware para abordar, entre otros problemas, nueve errores de seguridad que afectan a una amplia gama de modelos de enrutadores.

Estado

De los nueve fallos de seguridad, dos tienen una gravedad crítica y seis tienen una gravedad alta. Una vulnerabilidad está actualmente pendiente de análisis.

La lista de productos afectados son GT6, GT-AXE16000, GT-AX11000 PRO, GT-AXE11000, GT-AX6000, GT-AX11000, GS-AX5400, GS-AX3000, XT9, XT8, XT8 V2, RT-AX86U PRO, RT - AX86U, RT-AX86S, RT-AX82U, RT-AX58U, RT-AX3000, TUF-AX6000 y TUF-AX5400.

Encabezando la lista de correcciones están CVE-2018-1160 y CVE-2022-26376 , las cuales tienen una calificación de 9.8 de un máximo de 10 en el sistema de puntuación CVSS.

CVE-2018-1160 se refiere a un error de escritura fuera de los límites de casi cinco años en las versiones de Netatalk anteriores a la 3.1.12 que podría permitir que un atacante remoto no autenticado logre la ejecución de código arbitrario.

CVE-2022-26376 se ha descrito como una vulnerabilidad de corrupción de memoria en el firmware de Asuswrt que podría activarse mediante una solicitud HTTP especialmente diseñada.

Los otros siete defectos son los siguientes:

- CVE-2022-35401 (puntaje CVSS: 8.1): una vulnerabilidad de omisión de autenticación que podría permitir que un atacante envíe solicitudes HTTP maliciosas para obtener acceso administrativo completo al dispositivo.
- CVE-2022-38105 (puntaje CVSS: 7.5): una vulnerabilidad de divulgación de información que podría explotarse para acceder a información confidencial mediante el envío de paquetes de red especialmente diseñados.

- CVE-2022-38393 (puntaje CVSS: 7.5): una vulnerabilidad de denegación de servicio (DoS) que podría activarse al enviar un paquete de red especialmente diseñado.
- CVE-2022-46871 (puntaje CVSS: 8.8): el uso de una biblioteca libusrsctp desactualizada que podría abrir los dispositivos objetivo a otros ataques.
- CVE-2023-28702 (puntaje CVSS: 8.8): una falla de inyección de comandos que podría ser aprovechada por un atacante local para ejecutar comandos arbitrarios del sistema, interrumpir el sistema o cancelar el servicio.
- CVE-2023-28703 (puntaje CVSS: 7.2): una vulnerabilidad de desbordamiento de búfer basada en pila que podría ser aprovechada por un atacante con privilegios de administrador para ejecutar comandos arbitrarios del sistema, interrumpir el sistema o terminar el servicio.
- CVE-2023-31195 (puntuación CVSS: N/A): una falla de adversario en el medio (AitM) que podría conducir a un secuestro de la sesión de un usuario.

Remediación / Referencias

ASUS recomienda que los usuarios apliquen las últimas actualizaciones lo antes posible para mitigar los riesgos de seguridad. Como solución alternativa, aconseja a los usuarios que deshabiliten los servicios accesibles desde el lado de la WAN para evitar posibles intrusiones no deseadas.

Por mayor información acceder a:

https://nvd.nist.gov/vuln/detail/CVE-2018-1160

Conclusiones

Las noticias contenidas en este boletín advierten sobre las nuevas modalidades y distintos ataques utilizados por ciberdelincuentes para alterar documentación digitalizada, falsificando y afectando la autenticidad de los mismos.

Recomendamos estar atentos y mantenerse informados respecto al phishing y a otras modalidades de ingeniería social, ya que se observa un incremento constante de intentos de engañar a las víctimas, mediante correos que buscan suplantar instituciones de manera ilegítima para robar y manipular información sensible de los clientes.

Seguimos viendo la importancia de estar atentos a las nuevas amenazas emergentes y a la importancia de aplicar actualizaciones.

En este último tiempo la evolución de las amenazas de software se incrementa mes a mes, recomendamos seguir midiendo nuestros estados de ciberseguridad en los accesos críticos del negocio y las conexiones laterales que puedan surgir de exponer la información sobre los diferentes canales de datos.

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

¡Sigan protegiéndose!