Boletín de Ciberseguridad

Fecha de Publicación
06/06/2022- N.º 35

Mes de Junio
23/05/2022 - 06/06/2022

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 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 6 noticias de relevancia sobre vulnerabilidades tecnológicas.

Aquellas noticias a tener especial recaudo son las siguientes:

La vulnerabilidad crítica de UNISOC afecta a millones de teléfonos Android:

Se ha descubierto una falla de seguridad crítica en el conjunto de chips para teléfonos inteligentes de UNISOC que podría utilizarse como arma para interrumpir las comunicaciones de radio de un teléfono inteligente a través de un paquete con formato incorrecto.

Microsoft lanza soluciones alternativas para la vulnerabilidad de Office:

Microsoft publicó el lunes una guía para una falla de seguridad de día cero recientemente descubierta en su paquete de productividad de Office que podría explotarse para lograr la ejecución de código en los sistemas afectados.

Detallan una nueva vulnerabilidad que afecta al canal de Google Chrome:

Han surgido detalles sobre una vulnerabilidad crítica de ejecución remota de código recientemente parcheada en el motor V8 JavaScript y WebAssembly utilizado en los navegadores basados en Google Chrome y Chromium.

UNISOC	**La vulnerabilidad crítica de UNISOC afecta a millones de teléfonos Android**	CRÍTICO

Descripción

Se ha descubierto una falla de seguridad crítica en el conjunto de chips para teléfonos inteligentes de UNISOC que podría utilizarse como arma para interrumpir las comunicaciones de radio de un teléfono inteligente a través de un paquete con formato incorrecto.

Estado

Al problema ahora parcheado se le ha asignado el identificador CVE-2022-20210 y tiene una calificación de 9,4 sobre 10 en cuanto a gravedad en el sistema de calificación de vulnerabilidad CVSS.

En pocas palabras, la vulnerabilidad descubierta se relaciona con un caso de vulnerabilidad de desbordamiento de búfer en el componente que maneja los mensajes de Non-Access Stratum (NAS) en el firmware del módem, lo que resulta en una negación de servicio.

Remediación / Referencias

Para mitigar el riesgo, se recomienda que los usuarios actualicen sus dispositivos Android con el último software disponible cuando esté disponible como parte del Boletín de seguridad de Android de Google para junio de 2022.

Por mayor información acceder a:
https://source.android.com/security/bulletin/2022-05-01

Microsoft	Microsoft lanza soluciones alternativas para la vulnerabilidad de Office	CRÍTICO

Descripción

Microsoft publicó el lunes una guía para una falla de seguridad de día cero recientemente descubierta en su paquete de productividad de Office que podría explotarse para lograr la ejecución de código en los sistemas afectados.

Estado

La debilidad, ahora asignada con el identificador CVE-2022-30190, tiene una calificación de 7,8 sobre 10.
Las versiones de Microsoft Office Office 2013, Office 2016, Office 2019 y Office 2021, así como las ediciones Professional Plus, se ven afectadas.

La vulnerabilidad de Follina, que salió a la luz a fines de la semana pasada, involucró un exploit del mundo real que aprovechó la deficiencia en un documento de Word armado para ejecutar código PowerShell arbitrario haciendo uso del esquema URI "ms-msdt:". La muestra se subió a VirusTotal desde Bielorrusia.

Remediación / Referencias

Además de publicar reglas de detección para Microsoft Defender para Endpoint, se han ofrecido soluciones alternativas para deshabilitar el protocolo URL de MSDT a través de una modificación del Registro de Windows.

Por mayor información acceder a:
https://msrc-blog.microsoft.com/2022/05/30/guidance-for-cve-2022-30190-microsoft-support-diagnostic-tool-vulnerability/

Office	**Se detecta un nuevo exploit de día cero de Microsoft Office en estado salvaje**	CRÍTICO

Descripción

Se está llamando la atención sobre una falla de día cero en Microsoft Office que podría usarse para lograr la ejecución de código arbitrario en los sistemas Windows afectados.

Estado

La vulnerabilidad salió a la luz después de que un equipo de investigación de ciberseguridad independiente conocido como nao_sec descubriera un documento de Word (" 05-2022-0438.doc ") que se cargó en VirusTotal desde una dirección IP en Bielorrusia.

La vulnerabilidad conocida como "Follina", usa la función de plantilla remota de Word para recuperar un archivo HTML de un servidor, que luego usa el esquema URI "ms-msdt://" para desencadenar la vulnerabilidad (carga útil maliciosa).

Se dice que se ven afectadas varias versiones de Microsoft Office, incluidas Office, Office 2016 y Office 2021, aunque se espera que otras versiones también sean vulnerables.

Remediación / Referencias

Se recomienda la activación de la siguiente regla para evitar esta vulnerabilidad:
https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/attack-surface-reduction-rules-reference?view=o365-worldwide#block-all-office-applications-from-creating-child-processes

Otra opción, es renombrar o eliminar la siguiente clave de registro:
"HKEY_CLASSES_ROOT\ms-msdt"
Esto hará que cuando el documento malicioso se abra, Office no podrá invocar ms-msdt, lo que evitará que el malware no se ejecute

Para saber más invitamos a visitar el siguiente sitio:
https://blog.segu-info.com.ar/2022/05/follina-zero-day-en-office-sin-macros.html

android	**Microsoft encuentra errores en aplicaciones de dispositivos Android**	CRÍTICO

Descripción

Se han revelado cuatro vulnerabilidades de alta gravedad en un marco utilizado por aplicaciones del sistema Android preinstaladas con millones de descargas.

Estado

Los problemas, ahora resueltos por su desarrollador, podrían haber permitido potencialmente que los actores de amenazas realicen ataques remotos y locales o que se abuse de ellos como vectores para obtener información confidencial aprovechando sus amplios privilegios del sistema.

A las debilidades, que van desde la inyección de comandos hasta la escalada de privilegios locales, se les han asignado los identificadores CVE-2021-42598, CVE-2021-42599, CVE-2021-42600 y CVE-2021-42601, con puntajes CVSS entre 7.0 y 8.9.
Algunas de las aplicaciones afectadas son de grandes proveedores internacionales de servicios móviles como Telus, AT&T, Rogers, Freedom Mobile y Bell Canada.

- Comprobación de dispositivos de Mobile Klinik (com.telus.checkup)
- Ayuda del dispositivo (com.att.dh)
- MyRogers (com.fivemobile.myaccount)
- Freedom Device Care (com.freedom.mlp.uat), y
- Transferencia de contenido del dispositivo (com.ca.bell.contenttransfer)

Remediación / Referencias

Microsoft recomienda a los usuarios que busquen el paquete de la aplicación "com.mce.mceiotraceagent", una aplicación que puede haber sido instalada por talleres de reparación de teléfonos móviles, y que en el caso de encontrarla, que la eliminen.

Para saber más invitamos a visitar el siguiente sitio:
https://www.microsoft.com/security/blog/2022/05/27/android-apps-with-millions-of-downloads-exposed-to-high-severity-vulnerabilities/

Linux	EnemyBot explota las vulnerabilidades del servidor web, Android y CMS	CRÍTICO

Descripción

Una botnet naciente basada en Linux llamada Enemybot ha ampliado sus capacidades para incluir vulnerabilidades de seguridad recientemente reveladas en su arsenal para apuntar a servidores web, dispositivos Android y sistemas de administración de contenido (CMS).

Estado

Revelado por primera vez por Securonix en marzo y luego por Fortinet, Enemybot ha sido vinculado a un actor de amenazas rastreado como Keksec (también conocido como Kek Security, Necro y FreakOut), con ataques tempranos dirigidos a enrutadores de Seowon Intech, D-Link e iRZ.

Enemybot, que es capaz de llevar a cabo ataques DDoS, tiene sus orígenes en otras redes de bots como Mirai, Qbot, Zbot, Gafgyt y LolFMe. Un análisis de la última variante revela que se compone de cuatro componentes diferentes:

- Un módulo de Python para descargar dependencias y compilar el malware para diferentes arquitecturas de sistemas operativos
- La sección central de botnets
- Un segmento de ofuscación diseñado para codificar y decodificar las cadenas del malware.
- Una funcionalidad de comando y control para recibir comandos de ataque y obtener cargas útiles adicionales

El malware también cuenta con una función para el escaneo de direcciones IP vulnerables y una función "adb_infect", que abusa de la función Android Debug Bridge para el compromiso de dispositivos móviles.

Remediación / Referencias

Si bien se cree que esta campaña está en fases iniciales, la constante actualización que recibe el malware y la posibilidad de explotar múltiples vulnerabilidades permitiría a los hackers desplegar campañas masivas en el futuro cercano.

Para saber más invitamos a visitar el siguiente sitio:
https://csirtasobancaria.com/alertas-de-seguridad/nueva-actividad-maliciosa-relacionada-a-la-botnet-enemybot

	**Detallan una nueva vulnerabilidad que afecta al canal de Google Chrome**	CRÍTICO

Descripción

Han surgido detalles sobre una vulnerabilidad crítica de ejecución remota de código recientemente parcheada en el motor V8 JavaScript y WebAssembly utilizado en los navegadores basados en Google Chrome y Chromium.

Estado

Las fallas de uso después de liberar ocurren cuando se accede a la memoria liberada anteriormente, lo que induce un comportamiento indefinido y hace que un programa se bloquee, use datos corruptos o incluso logre la ejecución de código arbitrario.

Lo que es más preocupante es que la falla se puede explotar de forma remota a través de un sitio web especialmente diseñado para eludir las restricciones de seguridad y ejecutar código arbitrario para comprometer los sistemas objetivo.

Remediación / Referencias

Se aconseja a los usuarios de Chrome, que actualicen la última versión disponible del software.

Para saber más invitamos a visitar el siguiente sitio:
https://www.incibe.es/protege-tu-empresa/avisos-seguridad/vulnerabilidad-critica-el-navegador-google-chrome

Conclusiones

Nuevo boletín quincenal de noticias relacionadas a la ciberseguridad y a la protección de nuestros activos de información.
En esta oportunidad hemos destacado como las amenazas internacionales en este panorama globalizado nos afectan a todos. Estás amenazas globales empujan necesariamente la evolución en los trabajos de defensa de todas las organizaciones, trabajos que miden y priorizan los riesgos y consideran impactos posibles en nuestras infraestructuras.

Está competencia nos obliga a revisar, configurar y actualizar nuestros sistemas de información de manera periódica.
Esta periodicidad que siempre es evaluada según los activos de información a los cuales afecte, es ponderada por el riesgo que pueden generar las amenazas. Trabajar en reforzar la seguridad de los sistemas conlleva diversos esfuerzos, que no son solamente actualizaciones simples ya probadas por otros equipos de desarrolladores, sino que también implican el refuerzo o "hardening" apropiado para cada situación.
Estas configuraciones, hacen que las amenazas generales y particulares tengan una menor tasa de incidencia o impacto, ya que se mitigan por estos controles compensatorios y demás controles de seguridad.

Hoy día cualquier organización que utilice y mantenga datos informáticos, por más chica o grande que sea; requiere esfuerzos específicos y especializados para evitar inconvenientes con sus sistemas e información. Vemos diariamente desde personas que descuidan el valor de su información, y hasta cómo los actores de amenazas pueden actuar en su contra.
Hay que recordar que la seguridad de la información trabaja en que las organizaciones ganen sin perder. Entonces evitar las pérdidas nos permitirá generar un diferencial competitivo.
Cuanto menores sean las ventanas de exposición y oportunidad a vulnerabilidades conocidas y explotadas por los ciberdelincuentes modernos, es que estaremos dando lucha en el frente de batalla cibernético, que diariamente nos convoca.

Desde Datasec seguimos apoyando a través de productos y servicios de seguridad de la información a cientos de compañías, atentos y proactivos a las novedades. Seguiremos informando por más noticias en la próxima quincena de días.