SECURESOFT CORPORATION
e-Secure Consulting Group

Reporte Semanal de Ciberinteligencia Securesoft

Fecha:

23 de Junio del 2020

El presente documento contiene información para la comunidad de ciberseguridad.

Equipo de Ciberinteligencia
CIB-FOR-2020-002

Índice

1. Objetivo

El presente documento de inteligencia tiene como objetivo informar sobre las principales vulnerabilidades y amenazas que se han detectado en el ciberespacio.

2. Alcance

Este documento muestra el resumen, la fecha de publicación, CVE asociado y servicios afectados de vulnerabilidades y amenazas que se han hecho públicas en el transcurso del 09 de junio hasta el 24 de junio del 2020.

3. Amenazas

Boletín	2020-184
Asunto	NUEVO AVADDON RANSOMWARE
Emisión	10/06/2020
CVE	No tiene
Categoría	Ransomware
Severidad	Alta

Servicios Afectados

Sistema operativo Windows

Descripción

Avaddon se distribuye a través de correos electrónicos que usan temas como "Your new photo?" o "Do you like my photo?". Los atacantes detrás de esta nueva amenaza están que utilizan la botnet Phorphiex/Trik para distribuir los correos.

Estos correos vienen con un archivo .jpg que en verdad es un archivo malicioso JavaScript que pretende hacerse para por una imagen.

Cuando se ejecuta, el archivo adjunto JS inicia un comando de PowerShell y Bitsadmin para descargar el ejecutable del ransomware Avaddon en la carpeta Temp y ejecutarlo. Una vez que se ejecuta, cifra los archivos de la víctima y les agrega la extensión .avdn. En cada carpeta, que se ha visto afectada se crea un archivo denominado "[id] -readme.html", el valor id se sustituye por un valor numérico dado por el atacante, está en una nota de rescate que contiene un enlace a un sitio de pago TOR.

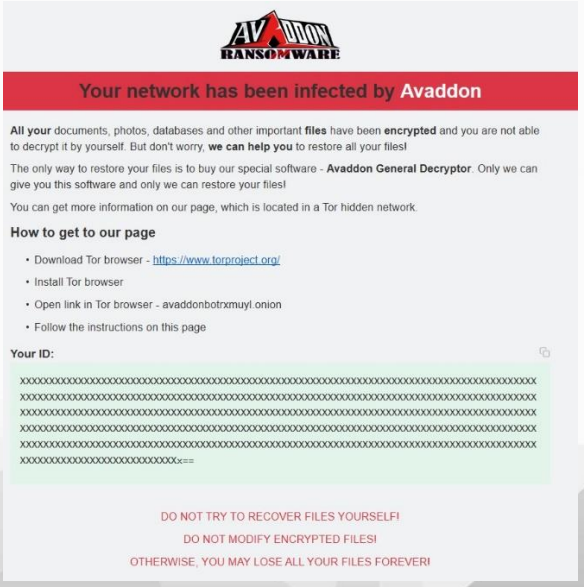

Imagen 1. Nota de rescate de Avaddon ransomware

Boletín	2020-185
Asunto	ACTUALIZACIÓN DE SEGURIDAD DE MICROSOFT - JUNIO 2020
Emisión	10/06/2020
CVE	Varios
Categoría	Vulnerabilidad
Severidad	Crítica

Servicios Afectados

Sistema operativo Windows

Descripción

En el mes de junio del 2020, Microsoft ha publicado actualizaciones para 130 vulnerabilidades. De las cuales 12 son consideradas como críticas y 118 como importantes.

En este paquete de actualizaciones Microsoft, entre las 12 vulnerabilidades críticas corregidas, 2 de ellas son del motor Microsoft Edge y VBScript, las cuales permiten a un atacante ejecutar código de manera remota y dañar la memoria del navegador. Las vulnerabilidades son CVE-2020-1216 y CVE-2020-1219 respectivamente.

Actualización o Mitigación

Se recomienda ver el contenido completo de esta noticia, para ello haga clic en el boletín que está en la tabla superior de esta página. En ese enlace encontrará mayor detalle de todas las vulnerabilidades junto con la actualización de cada vulnerabilidad.

Imagen 2. Logo de la marca del producto afectado

Boletín	2020-186
Asunto	THANOS RANSOMWARE INCLUYE CARACTERÍSTICA RIPLACE
Emisión	11/06/2020
CVE	No tiene
Categoría	Ransomware
Severidad	Alta

Servicios Afectados

Sistema operativo Windows

Descripción

Se identificó que Thanos se ofrece como un Ransomware como Servicio (RaaS, abreviado en inglés) en foros de atacantes de habla rusa desde febrero de 2020. Para mantenerse activo los operadores de este buscan otros atacantes y distribuidores de malware, el beneficio para estos últimos es un porcentaje del pago del rescate que la víctima da para tratar de recuperar su información.

La técnica RIPlace fue descubierta y comunicada de manera oportuna a distintos fabricantes de seguridad el año pasado. Se tiene información que las compañías Kaspersky y Carbon Black actualizaron su software para evitar esta técnica.

Al igual que otros ransomware, Thanos no solo encripta los archivos de la víctima sino que también los extrae y los envía a un servidor que se encuentra bajo el control de los atacantes, para ello usa la función ftp_file_exfil().

Hasta el momento se ha observado que este ransomware ha sido usado en ataques dirigidos a empresas en las que se cifraron varios servidores.

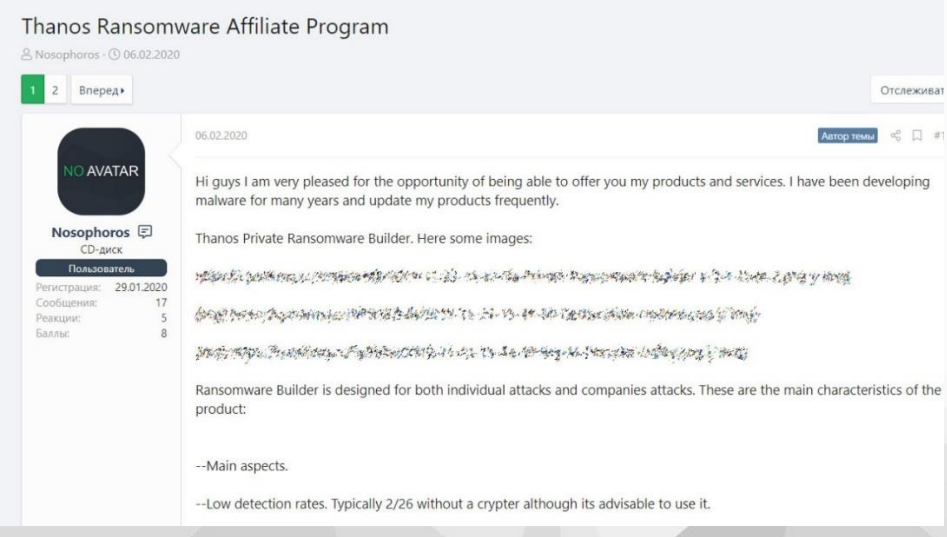

Imagen 3. Promoción del actor Nosophorus, para reclutar crackers y distribuidores del ransomware Thanos

Boletín	2020-187
Asunto	NUEVA CAMPAÑA DE TRICKBOT
Emisión	12/06/2020
CVE	No tiene
Categoría	Malware
Severidad	Alta

Servicios Afectados

Sistema operativo Windows

Descripción

Los atacantes suelen aprovecharse de temáticas actuales para engañar a sus víctimas, provocando que estas abran correos electrónicos maliciosos. Este es el caso de una actual campaña en la que se le pide a las víctimas que voten anónimamente sobre "Black Lives Matter" vía correo electrónico.

En el mensaje del correo se le sugiere a la víctima que descargue el archivo adjunto e-vote_form_3438.doc. Al descargar el archivo y ejecutarlo, se abrirá pidiéndole a la víctima que "Habilite la edición" y "Habilite el contenido". Una vez que se haya hecho clic en estos botones se ejecutarán macros que descargarán una DLL maliciosa en la computadora y la ejecutarán.

La DLL descargada es el troyano TrickBot, el cual descargará más módulos maliciosos en la computadora infectada, esto lo hace para poder robar archivos, contraseñas, propagarse lateralmente por la red y permitir que otros atacantes instalen ransomware.

Imagen 4. Imagen de referencia de la campaña que está siendo aprovechada por los atacantes

Boletín	2020-188
Asunto	RANSOMWARE BLACK KINGDOM APROVECHA VULNERABILIDAD EN PRODUCTOS DE PULSE SECURE
Emisión	15/06/2020
CVE	CVE-2019-11510
Categoría	Ransomware
Severidad	Crítica

Servicios Afectados

• Pulse Connect Secure de 8.1R1 a 8.1R15, de 8.2R1 a 8.2R12, de 8.3R1 a 8.3R7 y de 9.0R1 a 9.0R3.3

• Pulse Policy Secure de 5.1R1 a 5.1R15, de 5.2R1 a 5.2R12, de 5.3R1 a 5.3R12, de 5.4R1 a 5.4R7 y de 9.0R1 a 9.0R3.1

Descripción

Cibercriminales están explotando la vulnerabilidad asignada al CVE-2019-11510. Las compañías que no aplicaron las actualizaciones recomendadas por el fabricante poseen equipos que ejecutan versiones vulnerables, lo cual está siendo aprovechado por los operadores detrás de Black Kingdom.

Se observó que el ransomware establece su persistencia al hacerse pasar por una tarea programada legítima para Google Chrome. La tarea programada ejecuta un código de cadena codificado en Base64 en una ventana oculta de PowerShell para obtener un script llamado "reverse.ps1", el cual es usado para abrir un shell inverso en la computadora comprometida, el cual podría contener alguno de los productos vulnerables de Pulse Secure.

Actualización o Mitigación

Aplicar las actualizaciones proveídas por Pulse Secure de acuerdo al producto afectado, haciendo clic aquí.

Imagen 5. Imagen de referencia de la marca afectada

Boletín	2020-189
Asunto	VULNERABILIDADES EN E-BUSINESS SUITE DE ORACLE
Emisión	16/06/2020
CVE	CVE-2020-2586 y CVE-2020-2587
Categoría	Vulnerabilidad
Severidad	Crítica

Servicios Afectados

• Oracle E-Business Suite de 12.1.1 a 12.1.3

• Oracle E-Business Suite de 12.2.3 a 12.2.9

Descripción

Durante el año pasado se descubrieron varias vulnerabilidades en EBS. Algunos de estos fueron corregidos por la marca. Sin embargo, las vulnerabilidades denominadas BigDebIT, recién se solucionaron con las actualizaciones publicadas en enero de 2020.

Hasta el momento se estima que hay 1,500 implementaciones de EBS que están expuestas a internet, lo que las hace más susceptible a los ataques que explotan las vulnerabilidades de BigDebIT si las actualizaciones proveídas por la marca no están instaladas.

Un atacante que explota con éxito estas vulnerabilidades, los cuales han sido asignados a los CVE-2020-2586 y CVE-2020-2587, puede tomar el control del entorno EBS.

Se ha observado un escenario de explotación dirigido a la aplicación General Ledger, la cual es una herramienta de gestión financiera de EBS. Lo más llamativo de esto es que, los ciberdelincuentes pueden pasar por alto muchas soluciones de seguridad.

Actualización o Mitigación

Aplicar las actualizaciones de E-Business Suite de acuerdo con los productos afectados, haciendo clic aquí.

Boletín	2020-190
Asunto	ATAQUES DE CIBERESPIONAJE EN EUROPA Y ORIENTE MEDIO
Emisión	17/06/2020
CVE	No tiene
Categoría	Ataque cibernético
Severidad	Alta

Servicios Afectados

Sistema operativo Windows

Descripción

Se ha identificado que la campaña ha estado activa entre septiembre y diciembre de 2019, se sospecha que el grupo de atacante detrás de esta campaña es Lazarus.

Los atacantes crearon cuentas falsas de LinkedIn haciéndose pasar por representantes de Recursos Humanos de dos compañías conocidas en sector aeroespacial y de defensa.

Desde las cuentas falsas se enviaban ofertas de trabajo utilizando la función de mensajería de LinkedIn a las víctimas. Después de entablar comunicación con ellos, los atacantes enviaban unos archivos RAR protegidos con contraseña, que pretenden ser documentos PDF con detalles sobre el salario y el puesto de trabajo.

Cuando se descarga el archivo RAR y se descomprime, se observa un archivo LNK. Este archivo abre un PDF, el cual muestra información del salario y puesto de trabajo. En segundo plano se descarga un backdoor, el cual envía solicitudes a un servidor controlado por el atacante. Este también se usa para filtra los datos recopilados en forma de archivo RAR.

Boletín	2020-191
Asunto	ACTUALIZACIÓN DE VLC MEDIA PLAYER
Emisión	17/06/2020
CVE	CVE-2020-13428
Categoría	Vulnerabilidad
Severidad	Alta

Servicios Afectados

VLC Media Player versiones 3.0.10 y anteriores.

Descripción

VLC, es un reproductor multimedia que admite muchos formatos adicionales, sin descargar complementos adicionales.

La vulnerabilidad ha sido asignada al CVE-2020-13428, esta se debe a un desbordamiento de búfer en el paquete H23X de VLC, la explotación exitosa de esta vulnerabilidad permite a los atacantes ejecutar comandos con el mismo nivel que el usuario, víctima, si se explota adecuadamente. Para explotarla es necesaria crear un archivo especial que pueda engañar a la víctima para que lo abra con VLC.

Se sospecha que esta vulnerabilidad puedes usarse en conjunto con otras para filtrar información de la víctima. Hasta el momento no se han encontrado exploits que permitan a los atacantes aprovecharse de esta vulnerabilidad.

Actualización o Mitigación

Instalar la versión 3.0.11 de VLC, haciendo clic aquí.

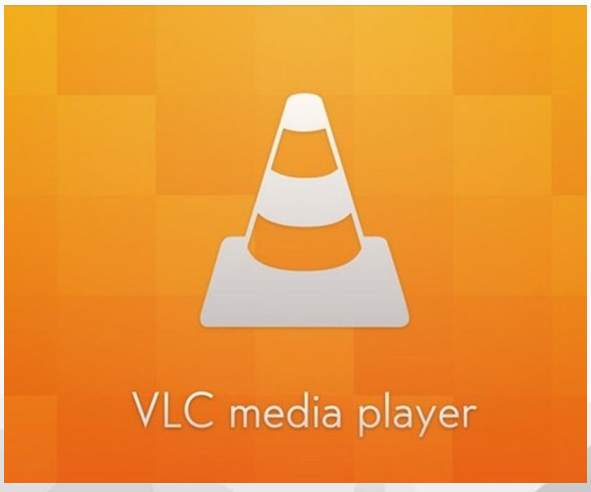

Imagen 6. Imagen de referencia del producto afectado

Boletín	2020-192
Asunto	VULNERABILIDAD DE CISCO WEBEX MEETINGS
Emisión	18/06/2020
CVE	CVE-2020-3347
Categoría	Vulnerabilidad
Severidad	Media

Servicios Afectados

Cisco Webex Meetings para Windows versiones anteriores a 40.6.0.

Descripción

La vulnerabilidad ha sido asignada al CVE-2020-3347, esta se debe al uso inseguro de la memoria compartida que el cliente de escritorio Cisco Webex Meetings emplea para intercambiar información con el sistema operativo Windows y otras aplicaciones en el sistema.

Este espacio de memoria compartida podría almacenar información confidencial, como tokens de autenticación, nombres de usuario e información de la reunión que podría ser obtenido por un usuario o proceso local malicioso. Luego esta puede ser usada para iniciar sesión con la cuenta WebEx de la víctima, ejecutar otro tipo de ataques; ver, editar y descargar reuniones, entre otras.

Se ha identificado que la vulnerabilidad afecta a los sistemas en los que la aplicación inicia de manera automática, la cual es la configuración predeterminada y común.

Actualización o Mitigación

Aplicar las actualizaciones proporcionadas por Cisco, las cuales se encuentran en el apartado Fixed Software, haciendo clic aquí.

Imagen 7. Imagen de referencia de la marca del producto afectado

Boletín	2020-193
Asunto	NUEVA VARIANTE DE HAKBIT RANSOMWARE
Emisión	18/06/2020
CVE	No tiene
Categoría	Ransomware
Severidad	Alta

Servicios Afectados

Sistema operativo Windows

Descripción

El ransomware es distribuido vía correo electrónico, el cual contiene un archivo Excel adjunto. Cuando la víctima descarga el Excel y hace clic en el botón "Habilitar contenido", se ejecutan macros maliciosas en la computadora.

El código macros ejecutado posee tres partes:

• La primera parte de la macro usa la función Workbook_Open(), la cual es usada para ejecutar la macro cuando Excel se ejecuta.

• La segunda parte usa un descifrador XOR declarada como función. Esta función contiene dos variables, las cuales son: "fine", que es la palabra clave y "job", que contiene los datos cifrados.

• La tercera parte realiza la parte principal de la función XOR declarada. Este va byte a byte a través de las cadenas ofuscadas y resta 7 del número ASCII para cada caracter. Una vez que se haya acabo con este proceso se devuelve una cadena de comandos, los cuales son usados para ejecutar PowerShell y descargar un archivo llamado client.exe, este crea un nuevo archivo llamado newfile.exe en la carpeta %Temp%.

Durante el análisis se observó que esta variante usa una técnica parecida a la de Ryuk ransomware para enviar un paquete Wake-On-Lan, la cual tiene por finalidad encriptar computadoras remotas en direcciones de subred locales específicas. Los archivos de las computadoras afectadas debido a esta técnica serán encriptados con un AES de 256 bits usando el modo CBC y encriptación RSA con una clave de 2048 bits.

Boletín	2020-194
Asunto	GOBIERNO Y ORGANIZACIONES AUSTRALIANAS BAJO ATAQUE
Emisión	19/06/2020
CVE	CVE-2019-0604, CVE-2019-18935 y CVE-2019-19781
Categoría	Ataque cibernético
Severidad	Crítica

Servicios Afectados

- Citrix
- Telerik
- SharePoint
- Microsoft Internet Information Services

Descripción

El gobierno australiano ha emitido un informe llamado "Copy-paste compromises", en español Compromisos de copiar y pegar. Esto debido a que se ha identificado que los atacantes usan el mismo código de explotación de Prueba de Concepto (PoC, por sus siglas en inglés), web shells y otras herramientas en distintos ataques.

Los ciberdelincuentes usan una serie de vectores de acceso iniciales, siendo la explotación de vulnerabilidades de infraestructura pública la más frecuente. Se observó que se aprovechan de vulnerabilidades de ejecución de código remoto en versiones no actualizadas de la interfaz de usuario de Telerik, Microsoft Internet Information Services (IIS), una vulnerabilidad de SharePoint 2019 y la vulnerabilidad Citrix 2019. Los CVE asignados a esas vulnerabilidades son: CVE-2019-0604, CVE-2019-18935 y CVE-2019-19781.

Si los atacantes no logran tener éxito con lo anteriormente mencionado, cambian de táctica y empiezan a utilizar diversas técnicas de spearphishing.

Una vez que los atacantes obtienen acceso inicial, usan una combinación de códigos maliciosos y herramientas personalizados para persistir e interactuar con la red de las víctimas.

Boletín	2020-195
Asunto	FILTRACIÓN DE DATOS POLICIALES EN EE.UU.
Emisión	22/06/2020
CVE	No tiene
Categoría	Filtración de datos
Severidad	Media

Servicios Afectados

Organizaciones policiales de los EE.UU.

Descripción

Los archivos fueron publicados por Negación de secretos distribuida (DDOS, por sus siglas en inglés), una organización tipo WikiLeaks que se describe a sí misma como un "colectivo de transparencia" cuyo objetivo es compartir información de interés público.

La filtración, denominada BlueLeaks, incluye archivos de más de 200 departamentos de policía, FBI y otras organizaciones policiales de varios estados de EE.UU.; estos incluyen imágenes, documentos, tablas, páginas web, archivos de texto, videos, archivos de audio y correos electrónicos.

Se ha publicado que la Asociación Nacional de Centros de Fusión (NFCA, por sus siglas en inglés) publicó que los datos fueron obtenidos de una empresa de desarrollo web con sede en Texas, llamada Netsential.

La NFCA también publicó que los archivos vulnerados tienen fechas desde 1996 hasta junio de 2020.

Hasta el momento se sabe que los cibercriminales comprometieron una cuenta de un cliente de Netsential y usaron esta para cargar un malware que les permitió obtener la información de otros clientes de Netsential, entre ellas organizaciones policiales.

Boletín	2020-196
Asunto	TRICKBOT IMPLEMENTA RYUK RANSOMWARE DESPUÉS DE DOS SEMANAS
Emisión	23/06/2020
CVE	No tiene
Categoría	Malware
Severidad	Alta

Servicios Afectados

Sistema operativo Windows

Descripción

Los atacantes detrás del troyano Trickbot, utilizan software de emulación de amenazas Cobalt Strike para Red Team, Equipo Rojo en español. Uno de los componentes utilizados es script DACheck, este permite verificar si el usuario afectado tiene privilegios de administrador de dominio, así como también encontrar otros miembros de este grupo. Por otro lado, se utilizó Mimikats para extraer contraseñas.

Se ha descubierto que los atacantes buscan computadoras con puertos específicos abiertos.

Los atacantes perfilan cada computadora infectada, esto les permite extraer una mayor cantidad de información, tomar control de la red y obtener acceso a tantas computadoras como sea posible.

Las etapas de reconocimiento y pivote son seguidas por la distribución e implementación de Ryuk ransomware, en todas las computadoras accesibles utilizando la herramienta PsExec de Microsoft para ejecutar procesos de forma remota.

Actualización o Mitigación

• Limitar el uso de PsExec de Microsoft solo ha a los administradores del sistema.

• Segmentar las redes internas de la organización mediante la implementación de VLANs.

Boletín	2020-197
Asunto	VULNERABILIDAD EN EL CLIENTE WINDOWS DE PULSE SECURE
Emisión	23/06/2020
CVE	No tiene
Categoría	Vulnerabilidad
Severidad	Alta

Servicios Afectados

• Pulse Secure Desktop client (Windows) versiones 5.3Rx, 9.0Rx, 9.1R5 y anteriores.

• Pulse Secure Installer Service (Windows) versiones 8.3Rx, 9.1Rx, 9.1R5 y anteriores.

Descripción

La vulnerabilidad asignada al CVE-2020-13162, afecta al cliente de Pulse Secure para Windows. Esta permite escalar privilegios locales en el servicio PulseSecureService.exe, la explotación de esta vulnerabilidad permite a un atacante aprovecharse del servicio anteriormente mencionado y ejecutar de manera arbitraria un Microsoft Installer con privilegios de SYSTEM, derechos más elevados de administración.

La vulnerabilidad radica en el componente dsInstallerService, en esta los usuarios sin privilegios de administrados pueden instalar o actualizar nuevos componentes utilizando instaladores proporcionados por Pulse Secure. Debido a que el componente realiza una verificación de firmas en el contenido del instalador. Se ha comprobado que es posible evadir esta verificación usando un instalador legítimo de Pulse Secure e intercambiándolo por un componente malicioso después de esta verificación. Permitiendo instalar programas maliciosos como backdoor, puerta trasera en español.

Actualización o Mitigación

Aplicar las actualizaciones recomendadas por Pulse Secure, haciendo clic aquí.

4. Recomendaciones

- Leer los boletines citados en las amenazas que tengan uno asociado, esto con la finalidad de encontrar más información de la amenaza como: Una mayor descripción, Indicadores de compromiso,recomendaciones personalizada y fuentes por amenaza.
- Considerar deshabilitar PowerShell y Macros de Microsoft, evitando que pueda ser aprovechado por softwares maliciosos.
- Utilizar una política de uso de contraseñas seguras considerando la complejidad, el cambio de credenciales por defecto y la no reutilización de las mismas.
- Mantener un protocolo estricto para realizar copias de seguridad de los activos de información de mayor criticidad.
- Mantener un protocolo de actualizaciones estricto de sistemas operativos, antivirus y todas las aplicaciones que se ejecutan en ellos.
- Bloquear los indicadores de compromisos (IOC) compartidos, en los dispositivos de seguridad de su infraestructura.
- Verificar la información de la cuenta que envía el correo, el nombre y la dirección del destinatario para identificar si son sospechosas.
- No abrir correos electrónicos de dudosa procedencia (remitente desconocido), ni dar clic en enlaces, ni descargar archivos adjuntos desconocidos.
- Escanear todo el software descargado de Internet antes de la ejecución.
- De detectar un correo spam, phishing o cualquier actividad anómala reportarlo. inmediatamente a los encargados de seguridad de la información de su institución.

* Antes de realizar el bloqueo de IOCs es importante que previamente en ambiente de desarrollo se valide y confirme a nivel de sus servicios internos y externos, con el propósito de aplicar los cambios de manera controlada.

** Es importante que previamente en ambiente de desarrollo se valide y confirme a nivel de los servicios, con el propósito de aplicar los cambios de manera controlada.