Boletín de Ciberseguridad

Fecha de Publicación
19/07/2021 - N.º 12

Mes de Julio
05/07/2021 - 19/07/2021

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 segunda quincena del mes de julio se destacan 6 noticias de relevancia: 2 sobre vulnerabilidades tecnológicas, 2 de fraudes activos y 2 de prevención.

Aquellas noticias a tener especial recaudo son las siguientes:

Errores críticos en productos Cisco
De las vulnerabilidades consideradas de riesgo crítico, se observa que, en el caso de una explotación exitosa un atacante puede usar un certificado que no corresponda a una autoridad certificadora como si lo fuera y firmar un certificado para una organización o usuario de manera arbitraria o para causar una condición de denegación de servicio (DoS).

Microsoft publica fallas críticas identificadas recientemente
Fuentes oficiales alertan por un gran número de fallas identificadas y publicadas por Microsoft, siendo una gran cantidad de ellas consideradas de riesgo crítico.

Fraude utilizando la doble autenticación de WhatsApp
Se ha observado anteriormente, distintas estrategias de phishing por WhatsApp implementadas por cibercriminales para vulnerar los dispositivos de sus víctimas. En este caso se trata de una estafa que mediante ingeniería social busca robar la credencial de activación del usuario, deshabilitando la contraseña personal que sirve como doble autenticación.

Utilización de documentos Office y macros como vector de ataque
Ha sido constatado en estrategias de Phishing anteriores, la distribución de archivos de Microsoft Office especialmente confeccionados, que solicitan a las víctimas habilitar macros para luego provocar la cadena de infección. Nuevos descubrimientos ponen en evidencia una nueva técnica utilizada por cibercriminales, que consiste en enviar documentos no maliciosos para deshabilitar las advertencias de seguridad, antes de ejecutar la macro para infectar a las víctimas.

CISCO	**Errores críticos en productos Cisco**	CRÍTICO

Descripción

Fuentes oficiales comparten información sobre errores críticos que afectan a diversos productos de la empresa de tecnología Cisco.

De las vulnerabilidades consideradas de riesgo crítico, se observa que, en el caso de una explotación exitosa un atacante puede usar un certificado que no corresponda a una autoridad certificadora como si lo fuera y firmar un certificado para una organización o usuario de manera arbitraria o para causar una condición de denegación de servicio (DoS).

Afectados

- Cisco BroadWorks Application Server
- Cisco Catalyst 4500 Series Switches
- Cisco Catalyst 4500-X Series Switches
- Cisco Web Security Appliance (WSA)

Estado

Actualmente no hay confirmación de que exista una explotación activa de estas vulnerabilidades, pero se insta a tomar en cuenta los siguientes errores detectados en la línea de productos Cisco.

Principales vulnerabilidades detectadas:
En la interfaz XSI-Actions de Cisco BroadWorks Application Server, lo que podría permitirá un usuario remoto autenticado acceder a información sensible en el sistema afectado.

En la implementación offload de Bidirectional Forwarding Detection (BFD) en switches Cisco Catalyst 4500 Series y 4500-X Series, lo que podría permitir a un atacante remoto no autenticado generar un colapso de los procesos iosd.

En la administración de configuración de Cisco AsyncOS para Cisco Web Security Appliance (WSA), lo que podría permitir a un atacante remoto no autenticado realizar inyección de comandos y elevar privilegios a root.

En la interfaz web de Cisco Business Process Automation (BPA), lo que podría permitir a un atacante autenticado remoto a elevar privilegios de Administrador.

Remediación / Referencias

Se recomienda instalar las respectivas actualizaciones desde el sitio web del proveedor.

Por mayor información acceder a:
https://www.csirt.gob.cl/vulnerabilidades/9vsa21-00465-01/
https://tools.cisco.com/security/center/publicationListing.x

Microsoft	Microsoft publica fallas críticas identificadas recientemente	CRÍTICO

Descripción

Fuentes oficiales alertan por un gran número de fallas identificadas y publicadas por Microsoft, siendo una gran cantidad de ellas consideradas de riesgo crítico.

Microsoft también lanzó actualizaciones a errores ya conocidos. Incluyendo un parche actualizado para una vulnerabilidad especialmente preocupante y que detallamos en profundidad en la edición del boletín Nro.11, conocida como PrintNightmare.

Afectados

- Windows Server 2004, 2008, 2012, 2012 R2, 2016, 2019, 20H2
- Microsoft Exchange Server 2013, 2016, 2019
- Microsoft Malware Protection Engine
- Microsoft Office 2013, 2013 RT, 2016, 2019
- Microsoft Office Online Server
- Microsoft Office Web Apps Server 2013

Para visualizar la lista completa de productos afectados, acceder al siguiente Link:
https://msrc.microsoft.com/update-guide

Estado

Principales vulnerabilidades detectadas:

De ejecución remota de código y afecta al scripting engine presente en cada versión de Windows aún con soporte.

De elevación de privilegios en el kernel de Windows, y están siendo explotadas.

Un error que permite la ejecución remota de código en las áreas más profundas del sistema operativo.

Vulnerabilidad en Windows DNS Server que alcanzó una clasificación CVSS de severidad de 9,8 de 10.

Remediación / Referencias

Para la vulnerabilidad de Microsoft PrintNightmare, en las recomendaciones nos gustaría informar que, para una mitigación rápida y efectiva, se debe deshabilitar el servicio de impresión.

A nivel de Windows vía PowerShell es posible realizarlo mediante el comando:

- Stop-Service -Name Spooler -Force

Otro comando es:

- Set-Service -Name Spooler -StartupType Disabled para deshabilitarlo por completo al reinicio. Esto se puede hacer tanto de forma local como por la GPO siguiendo los pasos de este enlace.
  https://www.windowscentral.com/how-mitigate-print-spooler-printnightmare-vulnerability-windows-10

Para corregir el resto de la fallas, invitamos a instalar las actualizaciones correspondientes desde el sitio web de Microsoft.

Por mayor información invitamos a visitar los siguientes sitios:
https://support.microsoft.com/es-es/windows/windows-update-preguntas-frecuentes-8a903416-6f45-0718-f5c7-375e92dddeb2
https://www.csirt.gob.cl/vulnerabilidades/9vsa21-00466-01/

Fraude utilizando la doble autenticación de WhatsApp

IMPORTANTE

Descripción

Se ha observado anteriormente, distintas estrategias de phishing implementadas por cibercriminales para vulnerar los dispositivos de sus víctimas. En este caso se trata de una estafa que mediante ingeniería social busca robar la credencial de activación del usuario, deshabilitando la contraseña personal que sirve como doble autenticación.

Una buena práctica de seguridad que ha sido recomendada por los especialistas, es la activación de la verificación de dos pasos, en la que el usuario crea una contraseña personal que se solicita en el momento de la instalación de la aplicación. Recientemente fue descubierto que mediante la utilización de Ingeniería Social se puede llegar a evadir este tipo de protección adicional.

Afectados

Usuarios de la aplicación de mensajería instantánea WhatsApp.

Desde su cuenta de Twitter, la app de Facebook informó que 2.000 millones de personas utilizan el servicio todos los meses. Además, todos los días se envían en promedio 100.000 millones de mensajes y se realizan 1.000 millones de llamadas.

Estado

En primer lugar, el usuario de la aplicación móvil recibe una llamada de parte del atacante simulando ser un funcionario de una institución médica reconocida pidiendo completar una encuesta. Al finalizar las preguntas, el delincuente le pide a la persona que comparta el código de autentificación de su celular, alegando que es para registrar su participación en la encuesta, evitando que la institución lo vuelva a llamar por lo mismo. Es ahí que la persona entrega sin saber información que puede dar acceso a su dispositivo a los atacantes.

Luego si los delincuentes observan que la cuenta de la víctima tiene habilitada la doble autenticación, el estafador llama a la víctima, haciéndose pasar por el equipo de soporte de WhatsApp explicando que se ha detectado actividad maliciosa en la cuenta. Después la persona recibe instrucciones de pedir el código y revisar su correo electrónico buscando el mensaje con el enlace que le permitirá registrarse de nuevo en la doble autenticación. Si la víctima no presta atención al mensaje y entrega el código, su cuenta podría ser expuesta.

Remediación / Referencias

Para evitar ser víctima, recomendamos:
Habilitar la autenticación de doble factor (código de seis dígitos) en WhatsApp.

- Ingrese a la opción "Configuración"
- Luego haga clic en "Cuenta"
- Seleccione "verificación de dos pasos"
- Cree un código de seis dígitos, el cual será su código de doble autenticación.
- Solicitar que su número de teléfono sea eliminado de listas de aplicaciones que identifican llamadas. Los estafadores pueden utilizar estas listas para encontrar su número a partir de su nombre.
- Nunca desactivar la autenticación de doble factor, a menos que olvide la contraseña y necesite cambiarla.

Por mayor información al respecto se puede acceder a:
https://blog.segu-info.com.ar/2021/07/robo-de-cuentas-en-whatsapp-al-burlar.html
https://latam.kaspersky.com/blog/robo-de-cuentas-en-whatsapp-al-burlar-la-doble-autenticacion/21962/
https://www.ambito.com/informacion-general/tecnologia/whatsapp-revelo-su-impactante-numero-usuarios-mes-n5172735

Utilización de documentos Office y macros como vector de ataque

IMPORTANTE

Descripción

Macros: es una serie de instrucciones que se almacenan para que se puedan ejecutar de manera secuencial mediante una sola llamada u orden de ejecución.

Ha sido constatado en estrategias de Phishing anteriores, la distribución de archivos de Microsoft Office especialmente confeccionados, que solicitan a las víctimas habilitar macros para luego provocar la cadena de infección. Nuevos descubrimientos ponen en evidencia una nueva técnica utilizada por cibercriminales, que consiste en enviar documentos no maliciosos para deshabilitar las advertencias de seguridad, antes de ejecutar la macro para infectar a las víctimas.

"Los investigadores de McAfee Labs encontraron una táctica novedosa que descarga y ejecuta una DLL maliciosos sin ningún código malicioso presente en la macro inicial que se distribuye mediante spam. El troyano ZLoader es un descendiente del infame troyano bancario ZeuS y es conocido por el uso agresivo de documentos de Office y macros como un vector de ataque inicial, para robar credenciales e información de identificación personal de los usuarios de las instituciones financieras específicas."

Afectados

Usuarios que utilizan distintos tipos de documentos de Microsoft Office.

"El software malicioso de macros (conocido también como el virus de macros o simplemente macro virus) es un nombre genérico para un tipo de infecciones informáticas que usan comandos macro de Microsoft Office. Los ciberdelincuentes diseñan documentos MS Office y hacen que se ejecuten comandos que descargarán e instalarán virus en el sistema. Casi siempre, tales documentos infecciosos se propagan usando campañas de spam."

Estado

El ataque comienza con el envío de un mail que contiene un archivo adjunto de Microsoft Word, que al ser abierto descarga un archivo de Microsoft Excel protegido con contraseña desde un servidor remoto. Las macros deben estar habilitadas en el archivo de Word para activar la descarga en sí.

"Después de descargar el archivo XLS, Word VBA lee el contenido de una celda desde el XLS y crea una nueva macro para el mismo archivo XLS y escribe el contenido de la celda en una nueva funciona, como macro. Una vez que las macros están escritas y listas, el documento de Word establece la política en el registro para "Desactivar la advertencia de macro de Excel" e invoca la

función de macro maliciosa desde el archivo de Excel. El archivo de Excel ahora descarga el payload de ZLoader y la DLL es ejecutada usando rundll32.exe."

Remediación / Referencias

Se advierte a tener especial atención por el avance de nuevos señuelos de ingeniería social que buscan vulnerar a quienes desconocen la temática.

Por mayor información al respecto se puede acceder a:
https://thehackernews.com/2021/07/hackers-use-new-trick-to-disable-macro.html
https://www.pcrisk.es/guias-de-desinfeccion/9078-macro-malware

Aplicaciones de aprendizaje para simular ataques DDoS

PREVENCIÓN

Descripción

A continuación, nos gustaría compartir algunas de las aplicaciones más importantes que pueden ser utilizadas para llevar a cabo simulaciones de ataques DDoS.

Se destaca su practicidad educativa para aprender más sobre el funcionamiento y protección ante este tipo de amenaza, además de su libre acceso ya que todos son gratuitos.

Afectados

Los ataques DoS se generan mediante la saturación de los puertos con múltiples flujos de información, haciendo que el servidor se sobrecargue y no pueda seguir prestando su servicio. Por eso se le denomina denegación, pues hace que el servidor no pueda atender la cantidad enorme de solicitudes.

"Una ampliación del ataque DoS es el llamado ataque de denegación de servicio distribuido, también llamado DDoS (por sus siglas en inglés, Distributed Denial of Service) el cual se lleva a cabo generando un gran flujo de información desde varios puntos de conexión hacia un mismo punto de destino. La forma más común de realizar un DDoS es a través de una red de bots, siendo esta técnica el ciberataque más usual y eficaz por su sencillez tecnológica."

Vector de Ataque

LOIC
Una de las herramientas que tenemos para simular un ataque DDoS y aprender sobre cómo nuestro sistema puede protegerse es LOIC. Son las siglas de Low Orbit Ion Cannon. Básicamente lo que hace este programa, que es de software libre y está disponible para Windows y Linux, es enviar una gran cantidad de paquetes TCP, UDP y peticiones HTTPS. Pone a prueba la red objetivo para ver hasta qué punto puede soportar este tipo de ataques

El objetivo de los desarrolladores de esta herramienta es que sirva para uso educativo. Pretenden que los usuarios puedan aprender más sobre cómo defenderse de ataques DDoS, ver si la defensa de los equipos es la adecuada y mejorar determinados parámetros.

HULK
Otro programa que podemos usar para el mismo propósito, para poner a prueba nuestros equipos y simular un ataque DDoS, es HULK. Es ideal para nuestros servidores web y ver hasta qué punto podrían soportar una amenaza de este tipo que pudiera dejar sin servicio a todos los visitantes que intenten acceder a nuestro sitio.

HULK son las siglas de HTTP Unbearable Load King. Esta herramienta está escrita en Python y permite generar una gran cantidad de peticiones únicas para afectar a la carga de un servidor. Lo podemos descargar también desde GitHub, donde veremos la información referente al código.

Tor's Hammer
Tor's Hammer también nos permite simular ataques DDoS. Permite poner a prueba servidores y aplicaciones. Su nombre no es casualidad, y es que permite utilizarlo a través de la red Tor para que sea totalmente anónimo.

El objetivo de este programa es saturar la pila TCP con múltiples solicitudes. Envía solicitudes incompletas, lentamente, para lograr mantener la conexión activa el mayor tiempo posible. Busca así provocar la denegación de servicio cuando el servidor ya no puede mantener más conexiones activas.

Estamos ante una herramienta escrita en Python y que podemos descargar desde GitHub.

BoNeSi
En este caso estamos ante un programa que funciona para Linux. Es de código abierto y totalmente gratuito que podemos ejecutar en la línea de comandos. Permite apuntar a una dirección IP y además lo podemos usar en una máquina virtual.

Como en los casos anteriores, con BoNeSi podemos poner a prueba nuestros servidores. Podemos ver hasta qué punto están capacitados para hacer frente a un ataque DDoS que pueda comprometer el buen funcionamiento. Una manera más de lograr una mejora importante en seguridad y tener un mayor conocimiento.

DDOSIM Layer 7
Este programa permite simular un ataque DDoS con múltiples direcciones IP aleatorias. Esto permite crear una gran cantidad de solicitudes TCP para apuntar a un servidor objetivo. Funciona de forma similar a BoNeSi y también lo podemos usar en Linux. Podemos descargar el código fuente desde GitHub y obtener allí toda la documentación necesaria.

El objetivo de DDOSIM Layer 7 no es otro que mostrarnos la capacidad real que tiene nuestro servidor para poder soportar posibles ataques de denegación de servicio que puedan recibir. Una manera más de preservar el buen funcionamiento y de evitar posibles problemas que sean aprovechados por los ciberdelincuentes para tumbar nuestras conexiones.

Remediación / Referencias

Mediante la concientización y utilización de los programas presentados anteriormente, se puede determinar hasta qué punto este tipo de ataques son soportados, contribuyendo a tomar las medidas de mitigación correspondientes que mejoran la seguridad de los usuarios.

Por mayor información al respecto se puede acceder a:
https://blog.segu-info.com.ar/2021/07/programas-para-simular-ataques-ddos.html
https://www.redeszone.net/tutoriales/seguridad/simular-ataques-ddos/

malicious software	Características del malware Bandook y su presencia en la región	PREVENCIÓN

Descripción

Se ha observado en 2021 distintitos ataques que apuntaban a redes corporativas en varios países de Latinoamérica, con el 90% de las detecciones en Venezuela. El malware utilizado es Bandook y se constató la aparición de nuevas funciones y otros cambios que se habían implementado en este malware ya conocido.

“Bandook es un RAT activo desde 2005. Su participación en diferentes campañas de espionaje, ya documentadas, nos muestra que sigue siendo una herramienta relevante para los cibercriminales. Además, si tenemos en cuenta las modificaciones realizadas al malware a lo largo de los años, nos muestra el interés de los ciberdelincuentes por seguir utilizando este malware en campañas maliciosas, haciéndolo más sofisticado y difícil de detectar.”

Afectados

Aunque hemos visto más de 200 detecciones para los droppers de este malware en Venezuela en 2021, no hemos identificado un sector en particular siendo apuntado por esta campaña. Según datos de nuestra telemetría los principales intereses de los atacantes son redes corporativas en Venezuela; algunas corresponden a empresas manufactureras, otras a sectores como la construcción, atención médica, servicios de software e incluso minoristas. Dadas las capacidades del malware y el tipo de información exfiltrada, parece que el objetivo principal es el espionaje. Sus víctimas y el método para abordarlas se parecen más a los de una operación de ciberdelito que a las actividades que realizan grupos de APT.

En 2021 solo se ha observado visto una campaña activa: la que apunta a países de habla hispana.

Vector de Ataque

Todo comienza con correos electrónicos que incluyen un archivo PDF malicioso como adjunto y que son enviados a los blancos de ataque. El archivo PDF contiene un enlace para descargar un archivo comprimido y la contraseña para extraerlo. Dentro del archivo hay un ejecutable: un dropper que inyecta Bandook en un proceso de Internet Explorer.

"Un dropper es un tipo de troyano cuyo propósito es instalar otro malware una vez que están presentes en un sistema. De hecho, se denominan trojan-dropper porque colocan malware y componentes de malware en un sistema comprometido."

Los atacantes utilizan acortadores de URL como Rebrandly o Bitly en los archivos PDF adjuntos que utilizan. Las URL abreviadas redirigen a servicios de almacenamiento en la nube, como Google Cloud Storage, SpiderOak o pCloud, desde donde se descarga el malware.

El contenido de los archivos PDF es genérico y se han utilizado varios nombres de archivo que cambian entre las víctimas

Remediación / Referencias

Recomendamos estar atentos a nuevas publicaciones referidas a las caracteristicas y avances de los malware mas peligrosos que persisten en la actualidad.

Por mayor información al respecto se puede acceder a:
https://www.welivesecurity.com/la-es/2021/07/07/campana-espionaje-america-latina-utiliza-malware-bandook/#:~:text=seguridad%20de%20ESET-,Bandidos%3A%20campa%C3%B1a%20de%20espionaje%20activa%20en%20Am%C3%A9rica%20Latina%20que%20utiliza,para%20espiar%20a%20sus%20v%C3%ADctimas

Conclusiones

En los sistemas internos de las organizaciones que protegemos, podemos medir y reconocer de forma centralizada el estado en que se encuentra el servicio de impresión en nuestros servidores. Determinando si son vulnerables a un posible compromiso por parte de la reciente vulnerabilidad descubierta conocida como "PrintNightmare". Para ello contamos con escaneos de vulnerabilidades internos o bien el listado y enumeración de los servicios a través de agentes de monitoreo, que se puede obtener mediante una herramienta de SIEM como Wazuh, Splunk, QRadar, Xabbix, etc.

A través de este tipo de reconocimiento podemos desplegar mitigaciones particulares sobre los sistemas afectados, a través de la ejecución de comandos que deshabiliten el servicio vulnerable que es el de impresión en este caso, que muchas veces está habilitado y no se utiliza. En otros casos la vía de resolución podría ser a través de la instalación de parches del sistema operativo Windows, lo que requiere en repetidas ocasiones de reinicios y parada de servicios del sistema. Esto provoca una alternancia de sucesos que a veces por las características del negocio dificultan estas tareas de mantenimiento, ya que se tiene que mantener la operativa con determinados niveles de servicio, tiempos, etc.

Tales dificultades suelen afrontarse con coordinación y planificación de las agendas de mantenimientos regulares, la misma debería sincronizar los momentos adecuados para implementar y alinear el tipo de servicio, de negocio, los operadores y los clientes asociados. Esto es parte de los procesos de gestión de ventanas de mantenimiento, que son agendadas con una determinada periodicidad. Donde algunos activos tendrán diferentes ciclos debido a su naturaleza, tomando en cuenta la gestión de sus pruebas e impactos, buscando lograr un balance adecuado entre la seguridad, las operaciones y los procesos del negocio.

Ayudamos a las organizaciones a través de distintos servicios de consultoría, servicios de defensa SOC, Hacking, entre otros, a facilitar y enfrentar con éxito los desafíos que se nos presentan diariamente.

Desde cada organización es posible impulsar hábitos seguros con el liderazgo adecuado, por eso debemos concientizar sobre los riesgos de seguridad existentes. Promoviendo hábitos y comportamientos que guíen de forma sistemática el ciclo de control de parches e instalación de actualizaciones en tiempo mínimos.

Los nuevos avances y la capacitación constante sobre Ciberseguridad son compromisos que asumimos e impulsamos a todos nuestros integrantes y colaboradores. También reconocemos la evolución que hemos logrado de forma efectiva en la protección proactiva de nuestros clientes, y celebramos con orgullo día a día esta noble tarea.

¡Datasec queda a su entera disposición y los invitamos a seguir protegiéndonos!