Boletín de Ciberseguridad

Fecha de Publicación
24/05/2021 - N.º 8

Mes de Mayo
10/05/2021 - 24/05/2021

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 mayo se destacan 6 noticias de relevancia: 3 sobre vulnerabilidades tecnológicas, 2 de fraudes activos y 1 de prevención.

Aquellas noticias a tener especial recaudo son las siguientes:

Se publican fallas de consideración en Adobe
“Han sido publicadas fallas de consideración critica en el programa Adobe y en una gran cantidad de sus productos. Se trata de más de 40 errores que repercuten tanto en equipos con sistemas operativos Windows como macOS.”

Error Zero-Day en IIS de Windows 10
“Mediante una Prueba de Concepto un especialista en seguridad informática realizo el exploit de una vulnerabilidad Zero-Day en el servidor web de Windows, Internet Information Services (IIS). El error, recibió una calificación de gravedad de 9,8 sobre 10”

Empresas pagan a banda de Ransomware una suma millonaria en Bitcoins
“El grupo criminal DarkSide cobro más de USD 10.000.000 en Bitcoin, extorsionado a dos grandes empresas, COLONIAL PIPELINE dedicada al transporte de gasolina y Brenntang que está orientada a la distribución de productos químicos. La amenaza se basó en la filtración publica de información robada.”

Empresas solucionan vulnerabilidades Zero-Days
“Microsoft ha corregido más de 55 fallas en su sistema, cuatro de ellas consideradas como críticas, 50 como importantes y una de valoración moderada.”

Adobe	**Se publican fallas de consideración en Adobe**	CRÍTICO

Descripción

Han sido publicadas fallas de consideración critica en el programa Adobe y en una gran cantidad de sus productos. Se trata de más de 40 errores que repercuten tanto en equipos con sistemas operativos Windows como macOS.

En el caso de que un atacante lleve a cabo con éxito el exploit, puede realizar la ejecución de código de forma remota (RCE), obtener una escalada de privilegios dentro del dispositivo accediendo a información confidencial del usuario.

Afectados

Lista completa de productos y versiones afectadas:
Adobe Experience Manager versión 6.5.7.0 y anteriores en todas sus plataformas.
Adobe Experience Manager versión 6.4.8.3 y anteriores en todas sus plataformas.
Adobe InDesign versión 16.0 y anteriores en sistemas operativos Windows.
Adobe Illustrator 2021 versión 25.2 y anteriores en sistemas operativos Windows.
Adobe InCopy versión 16.0 y anteriores en sistemas operativos Windows.
Adobe Acrobat DC y Adobe Acrobat Reader versión 2021.001.20150 y anteriores en sistemas operativos Windows.

Adobe Acrobat DC y Adobe Acrobat Reader versión 2021.001.20149 y anteriores en sistemas operativos macOS.
Adobe Acrobat 2020 y Adobe Acrobat Reader 2020 versión 2020.001.30020 y anteriores en sistemas operativos Windows y macOS.
Adobe Acrobat 2017 y Adobe Acrobat Reader 2017 versión 2017.011.30194 y anteriores en sistemas operativos Windows y macOS.
Adobe Creative Cloud versión 5.3 y anteriores en sistemas operativos Windows.
Adobe After Effects versión 18.1 y anteriores en sistemas operativos Windows.
Adobe Medium versión 2.4.5.331 y anteriores en Oculus.
Adobe Animate versión 21.0.5 y anteriores en sistemas operativos Windows.

Estado

"Entre los fallos notificados destaca la vulnerabilidad de tipo zero-day en Adobe Acrobat y Adobe Reader la cual aprovecha un error de tipo Use-After-Free (uso de memoria previamente liberada, pudiendo provocar una denegación de servicio, una filtración de memoria e incluso ejecución de código). "

Adobe ha confirmado que esta falla está siendo explotada actualmente en dispositivos Windows.

A continuación, algunos de los productos más populares con vulnerabilidades catalogadas por el fabricante como críticas:

Adobe Acrobat y Adobe Reader - Ejecución de código de forma remota.
Adobe InDesign - Ejecución de código de forma remota.
Adobe Illustrator - Ejecución de código de forma remota.
Adobe Creative Cloud Desktop Application - Ejecución de código de forma remota.
Adobe Creative Cloud Desktop Application - Ejecución de código de forma remota.
Adobe After Effects - Ejecución de código de forma remota.

Remediación / Referencias

Recomendamos a los usuarios y administradores de sistemas que utilizan Adobe, aplicar las actualizaciones de seguridad con el fin de prevenir y evitar la posibilidad de ataques futuros.

Por mayor información acceder a:
https://helpx.adobe.com/security.html
https://www.ccn-cert.cni.es/seguridad-al-dia/avisos-ccn-cert/11000-ccn-cert-av-16-21-vulnerabilidades-en-adobe.html

Microsoft IIS	Error Zero-Day en IIS de Windows 10	CRÍTICO

Descripción

Mediante una Prueba de Concepto un especialista en seguridad informática realizo el exploit de una vulnerabilidad Zero-Day en el servidor web de Windows, Internet Information Services (IIS).

En seguridad informática, se usan pruebas de concepto para explicar cómo se pueden explotar vulnerabilidades de día cero. Se trata de vulnerabilidades que se desconoce su funcionamiento exacto, y por tanto se utilizan PoC para intentar entender cómo pueden explotarse en un sistema o equipo.

"El error, que recibió una calificación de gravedad de 9,8 sobre 10, es una vulnerabilidad de corrupción de memoria en la pila del protocolo HTTP (http.sys) incluida en las versiones recientes de Windows. Esta pila es utilizada por el servidor IIS integrado de Windows y, si este servidor está habilitado, Microsoft dice que un atacante puede enviar un paquete con formato incorrecto y ejecutar código malicioso directamente en el kernel del sistema operativo."

Afectados

Servidor web de Windows: Internet Information Services (IIS).

Versiones recientes de Windows: Windows 10 2004 y 20H2, y Windows Server 2004 y 20H2, que básicamente incluye las versiones del sistema operativo Windows 10 y Windows Server lanzadas el año 2020.

Se estima que este servidor tiene más de 688 millones de instalaciones descargadas, seguidos por Nginx con 358 millones y Apache con 313 millones.

Estado

La explotación de esta vulnerabilidad no se logró concretar por los ciberdelincuentes ya que su resultado y conclusión es debió a una Prueba de Concepto, cuya finalidad es poner al descubierto errores aun no descubiertos, para poder tomar medidas preventivas y de corrección en el programa.

Microsoft pone de manifiesto que esta falla podría usarse para crear gusanos de red que se repliquen de un servidor a otro.

Remediación / Referencias

Esta vulnerabilidad fue corregida en las actualizaciones de este mes de mayo 2021. Se insta a realizar las actualizaciones correspondientes.

Por mayor información invitamos a visitar los siguientes sitios:
https://blog.segu-info.com.ar/2021/05/vulnerabilidad-critica-en-iis-de.html
https://therecord.media/poc-released-for-wormable-windows-iis-bug/amp/

Vulnerabilidad que permite el seguimiento de usuarios en varios buscadores

IMPORTANTE

Descripción

Fue publicada una vulnerabilidad que funciona en los navegadores de escritorio más populares por su uso (Chrome, Firefox, Safari y Tor Browser). El error se denominó como Scheme Flooding y permite el seguimiento de los usuarios, significando una violación a la privacidad.

La modalidad para el exploit de esta vulnerabilidad es llamada como "inundación de esquema", esta puede crear un identificador único, vinculando al navegador con la identidad del usuario para luego rastrear los movimientos del usuario dentro de Internet.

El proceso de identificación dura muy poco tiempo y es aplicable en equipos con sistemas operativos muy utilizados a nivel de escritorio, como Mac, Windows y Linux

"Nos referiremos a esta vulnerabilidad como inundación de esquemas, ya que utiliza esquemas de URL personalizados como vector de ataque. La vulnerabilidad utiliza información sobre las aplicaciones instaladas en la computadora para asignarle un identificador único permanente, incluso si cambia de navegador, usa el modo de incógnito o se utiliza una VPN."

Afectados

Especialistas en ciberseguridad han determinado que este exploit ha sido exitoso en buscadores como Chrome, Firefox, Safari y Tor, entre otros. Se considera que los navegadores más inseguros a esta vulnerabilidad son Safari y Tor.

Estado

Dependiendo del navegador varia la implantación del exploit, pero la idea a nivel general es la misma. Esto funciona solicitando al buscador que muestre un cuadro de dialogo de confirmación en una ventana emergente. Después mediante un código Java Script se puede detectar si se abrió la ventana emergente, detectando la presencia de una aplicación.

"Además, esta vulnerabilidad permite crear publicidad dirigida según los perfiles de los usuarios y sin su consentimiento. La lista de aplicaciones instaladas en el dispositivo puede revelar mucho sobre su ocupación, hábitos y edad. Por ejemplo, si se encuentra instalado un IDE de Python o un servidor PostgreSQL, es muy probable que sea un desarrollador de backend."

Remediación / Referencias

Actualmente se sabe que la falla data de al menos 5 años y está presente en todos los buscadores antes nombrados, desconociendo el impacto que ha tenido hasta el momento.

"Dependiendo de las aplicaciones instaladas en un dispositivo, es posible que un sitio web identifique a personas con fines más siniestros. Por ejemplo, un sitio puede detectar a un oficial del gobierno o militar en Internet en función de sus aplicaciones instaladas y el historial de navegación asociado que está destinado a ser anónimo."

Es debido a esto que se debe estar muy atento a nuevas modalidades de ingeniería social y a las remediaciones correspondientes que sean publicadas por especialistas en seguridad informática.

Por mayor información invitamos a visitar los siguientes sitios:
https://blog.segu-info.com.ar/2021/05/scheme-flooding-vulnerabilidad-que.html
https://fingerprintjs.com/blog/external-protocol-flooding/

	**Empresas pagan a banda de Ransomware una suma millonaria en Bitcoins**	CRÍTICO

Descripción

El grupo criminal DarkSide cobro más de USD 10.000.000 en Bitcoin, extorsionado a dos grandes empresas, COLONIAL PIPELINE dedicada al transporte de gasolina y Brenntang que está orientada a la distribución de productos químicos. La amenaza se basó en la filtración publica de información robada.

Se sabe con seguridad que Brenntang efectuó el pago y se estima que COLONIAL PIPELINE también habría realizado un pago en Bitcoins de similar suma por poder seguir con su correcta operativa, ya que el daño efectuado repercutió de gran manera a distintas líneas de transporte utilizadas.

Afectados

Brenntag: Se trata de una empresa alemana de distribución de productos químicos fundada en 1874 en Berlín. La compañía tiene su sede en Essen, Alemania y tiene operaciones en más de 77 países en todo el mundo.

COLONIAL PIPELINE: Empresa operadora del mayor oleoducto de combustible, diariamente transporta más de 100 millones de galones de gasolina, diésel, combustible para calefacción doméstica y combustible para aviones, conectando refinerías de Texas con Nueva York a través de la Costa Este de Estados Unidos,

Estado

El ataque contra Colonial, obligó a la empresa a desconectar sus sistemas, luego de lo cual ha logrado restablecer algunas líneas menores.

"Las fuentes dijeron que Colonial sintió una inmensa presión para que la gasolina y el combustible para aviones volvieran a fluir hacia las principales ciudades estadounidenses. Una tercera persona familiarizada con la situación dijo que los funcionarios del gobierno estadounidense están al tanto de que Colonial realizó el pago. El miércoles 12, el Washington Post y Reuters habían informado de que "la empresa no tenía intención inmediata de pagar el rescate", a pesar de que había pagado días antes."

Después de que se efectuara el pago los atacantes proporcionaron a Brenntag una herramienta de descifrado para que fuera restaurada su red informática, la cual estaba inhabilitada.

Además, se hizo público que la herramienta de descifrado era muy lenta y por lo tanto se debió seguir con el proceso manual de recuperación de backup. Debido a esto la empresa siguió utilizando sus propias copias de seguridad para ayudar a restaurar el sistema.

Remediación / Referencias

Por mayor información al respecto se puede acceder a:
https://blog.segu-info.com.ar/2021/05/colonial-pipeline-y-la-petroquimica.html
https://www.cnet.com/news/colonial-pipeline-reportedly-paid-5m-to-hackers-after-ransomware-attack/

Banco de Chile	Quedó al descubierto sitio web que suplanta al Banco de Chile	IMPORTANTE

Descripción

Se ha identificado un sitio web falso que se hace pasar por el Banco de Chile. En un claro intento de phishing, lo que podría servir para robar información sensible de los clientes como credenciales de usuarios, datos personales, etc.

En el caso de que los cibercriminales logren cumplir el objetivo de vulnerar la confidencialidad de usuarios y funcionarios del banco, podría tener una gran repercusión afectando la marca e imagen institucional del banco.

Afectados

Banco de Chile: "Se trata de una institución financiera que opera en Chile. Cuenta con una red de sucursales presentes en gran parte del país, cajeros automáticos y otros canales de distribución electrónicos. Proporciona productos y servicios financieros a grandes corporaciones, pequeñas y medianas empresas, y a personas. Sus cajeros automáticos se encuentran conectados a la red interbancaria Redbanc, la cual el banco controla un 38,13% de su propiedad."

En cuanto a la cantidad de usuarios, Banco de Chile se encuentra posicionado en el segundo puesto, con más de 900.000 cuentas corrientes activas. En el primer lugar se encuentra Banco Santander con algo más de 1.000.000.

Estado

Indicadores de compromiso

URL sitio falso
http://login.bancochile.maaherbuilders.com[.]pk/1621353328/bcochile-web/persona/login/index.html/login

Datos Alojamiento

IP: [51.195.206.62]
Número de Sistema Autónomo (AS): 16276
Etiqueta del Sistema Autónomo: OVH SAS
País: FR
Registrador: EU

Datos del Dominio

Nombre de Dominio: maaherbuilders.com.pk
Creado: 04-06-2017
Expira: 04-06-2023

Información del Registrador: NIC Chile
ID IANA: NO APLICA
Correo Electrónico: NO APLICA
Name Server: ukvip22.noc40.com
ukvip21.noc40.com

Remediación / Referencias

Recomendaciones a tener en cuenta:

- No abrir correos ni mensajes de dudosa procedencia.
- Desconfiar de los enlaces y archivos en los mensajes o correo.
- Mantener actualizadas sus plataformas (Office, Windows, Adobe Acrobat, Oracle Java y otras).
- Ser escépticos frente ofertas, promociones o premios increíbles que se ofrecen por internet
- Prestar atención en los detalles de los mensajes o redes sociales
- Evaluar el bloqueo preventivo de los indicadores de compromisos.
- Mantener actualizadas todas las plataformas de tecnologías y de detección de amenazas.
- Revisar los controles de seguridad de los AntiSpam y SandBoxing.
- Realizar concientización permanente para los usuarios sobre este tipo de amenazas.
- Visualizar los sitios web que se ingresen sean los oficiales.

Por mayor información al respecto se puede acceder a:
https://blog.segu-info.com.ar/2021/05/colonial-pipeline-y-la-petroquimica.html

El informe oficial publicado por el CSIRT del Gobierno de Chile está disponible en el siguiente enlace:
https://www.csirt.gob.cl/media/2021/05/8FFR21-00952-01.pdf

	**Empresas solucionan vulnerabilidades Zero-Days**	PREVENCIÓN

Descripción

Microsoft ha corregido más de 55 fallas en su sistema, cuatro de ellas consideradas como críticas, 50 como importantes y una de valoración moderada.

Afectados

Empresas: Microsoft, Adobe, Apple, CISCO, SAP, VMware.

Vector de Ataque

Vulnerabilidades Críticas:
HTTP.sys Protocol Stack – Ejecución de Código Remoto
Scripting Engine – Corrupción de Memoria - Internet Explorer.
Ejecución de Código Remoto en Hyper-V

Otras vulnerabilidades importantes a tener en cuenta:
NET and Visual Studio – Vulnerabilidad de Elevación de Privilegios.
Cinco vulnerabilidades en Microsoft Exchange Server Security Feature Bypass Vulnerability.
Common Utilities Remote Code Execution. Esta vulnerabilidad es para el kit de herramientas NNI. (Neural Network Intelligence) de Microsoft y fue revelada por Abhiram V de Resec System en GitHub.

Remediación / Referencias

"Se espera que los actores de amenazas analicen los parches para crear exploits para las vulnerabilidades, especialmente la de Microsoft Exchange. Por lo tanto, es vital aplicar las actualizaciones de seguridad lo antes posible."

Actualizaciones recientes:
Las actualizaciones de seguridad de mayo de Android se lanzaron la semana pasada.

Adobe lanzó actualizaciones de seguridad para Adobe Creative Cloud Desktop, Framemaker y Connect. Especialmente una vulnerabilidad use-after-free que se ha estado explotando en Windows.

Apple lanzó actualizaciones de seguridad para iOS, macOS, iPadOS, watchOS y Safari que corrigieron las vulnerabilidades de Webkit explotadas activamente.

Cisco lanzó actualizaciones de seguridad para numerosos productos este mes.

SAP lanzó sus actualizaciones de seguridad de mayo de 2021.

VMware lanzó actualizaciones de seguridad en mayo.

Por mayor información al respecto se puede acceder a:
https://blog.segu-info.com.ar/2021/05/microsoft-adobe-apple-cisco-sap-vmware.html
https://www.bleepingcomputer.com/news/microsoft/microsoft-may-2021-patch-tuesday-fixes-55-flaws-3-zero-days/amp/

Conclusiones

En esta oportunidad se reabre el debate tanto sobre la gestión de seguridad en infraestructuras y servicios críticos de las naciones y las cadenas de abastecimiento de productos y valores que sostienen la vida moderna tal y como la conocemos. Además de como la fuerte necesidad de las mismas es aprovechada por actores maliciosos, para extorsionar y que a estas organizaciones nos les "quede otra" que pagar por la extorsión de los datos cifrados a través de los virus tipo Ransomware que infectaron centros de datos.

La noticia particularmente del ataque a la empresa Colonial Pipeline, de transporte de combustibles recientemente en U.S.A. han visto que la seguridad industrial y de la cadena de suministros es un trabajo muy difícil de ejecutar y hacer seguimiento, la confianza entre varios actores y funciones requiere validaciones que no en todos los equipos y circunstancias existen y esto tanto por razones tecnológicas como a veces políticas.

Existen varios informes en dónde aproximadamente menos del 30% de empresas españolas reconocen contar con un buen inventario y gestión de activos de información, y que claramente es por dónde deberían comenzar a identificar para reconocer riesgos y luego aplicar eventuales mejoras. Como dato alentador tenemos que según encuestas varias cerca del 89% de las empresas energéticas son conscientes de las necesidades de invertir en ciberseguridad y lo están incorporando en sus planes estratégicos.

El impacto de este ataque particular fue tal, que cerca del 60% de estaciones de servicio y distribución de combustibles de al menos 3 estados no pudieran abastecer a sus clientes. Se requiere además una serie de renovaciones tecnológicas que son necesarias de ser evaluadas y priorizadamente descartadas e intercambiadas por otros componentes, esto es una ardua tarea.

En la actualidad, los ataques cibernéticos a la cadena de suministro de las empresas han aumentado un 78% en tan solo un año. Los ataques pueden incluir manipulación, sabotaje, falsificación, piratería, robo, destrucción, alteración, desviación, corrupción, ingeniería social o incluso amenazas internas.

La mayoría de estos ataques cibernéticos afectan a los correos electrónicos con archivos Office adjuntos. Es por eso que desde Datasec recomendamos para evitar estos ataques, y reducir los riesgos en los entornos industriales y de infraestructuras críticas, es trabajar en el ajuste de los procesos de ciberseguridad a través análisis de vulnerabilidades y riesgos, procesos de actualización o protección de componentes tecnológicos, no solo como evaluaciones internas, sino que además de la confianza y garantías con nuestros proveedores de software y hardware.

Trabajando más en la prevención es que se ahorran costes importantes en pagos a delincuentes por medios de extorsión entre otros. Cuídense!