Boletín de Ciberseguridad

Fecha de Publicación
30/08/2021 - N.º 15

Mes de Agosto
16/08/2021 - 30/08/2021

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 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 segunda quincena del mes de agosto se destacan 6 noticias de relevancia: 4 sobre vulnerabilidades tecnológicas, 1 de fraude activos y 1 de prevención.

Aquellas noticias a tener especial recaudo son las siguientes:

Miles de servidores de Microsoft Exchange son infectados por un Backdoor

Especialistas en ciberseguridad alertan sobre un hackeo reciente a miles de servidores de Microsoft Exchange, los cuales fueron infectados mediante un backdoor. Se cree que esto es debido a la falta de actualizaciones por parte de los usuarios para la familia de fallas conocidas como ProxyShell.

Dispositivos IoT son comprometidos por fallas de seguridad

Fuentes oficiales publican una falla de consideración crítica que afecta a millones de dispositivos IoT que utilizan la red ThroughTek "Kalay".

En publicaciones anteriores hemos explicado los problemas de seguridad que pueden presentar este tipo de dispositivos, muchos de tipo doméstico, que, al estar conectados a la red, son permeables a ser vulnerados pudiendo dejar expuesta información sensible de los usuarios.

IISerpent: un malware que manipula el resultado de los navegadores

Especialistas alertan sobre un intento de fraude mediante un troyano que se ubica de lado del servidor y que tiene como objetivo alterar los resultados de búsqueda de los distintos navegadores de Internet, a través del secuestro de reputación de los sitios web que compromete.

	Miles de servidores de Microsoft Exchange son infectados por un Backdoor	CRÍTICO

Descripción

Especialistas en ciberseguridad alertan sobre un hackeo reciente a miles de servidores de Microsoft Exchange, los cuales fueron infectados mediante un backdoor. Se cree que esto es debido a la falta de actualizaciones por parte de los usuarios para la familia de fallas conocidas como ProxyShell.

Los primeros ataques fueron reportados luego que se publicara en Internet, una prueba de concepto (PoC) a principios de mes con el código de explotación correspondiente. En las últimas semanas se observó un incremento significativo de los ataques bajo esta modalidad.

Afectados

Son alrededor de 1900 los servidores de Microsoft Exchange vulnerados y se detectó que más de 30.400 servidores Exchange de un total de 100.000 equipos analizados, aún no han sido actualizados, por lo que aún está latente el riesgo de que este ataque se siga perpetuando si no se toman las medidas de remediación necesarias.

Estado

ProxyShell: se trata de un grupo o familia compuesto por tres vulnerabilidades diferentes de seguridad, que les permite a los atacantes tomar el control de los servidores de correo electrónico de Microsoft Exchange.

La primera falla proporciona un mecanismo para la ejecución remota de código previo a la autenticación, lo que permite a los actores malintencionados ejecutar código de forma remota en un sistema afectado.

La segunda falla permite que los actores malintencionados ejecuten código arbitrario después de la autenticación en los servidores de Microsoft Exchange debido a una falla en el servicio PowerShell que no valida adecuadamente los tokens de acceso.

La tercera falla permite a los actores malintencionados, posteriormente a la autenticación ejecutar código arbitrario en el contexto de SYSTEM y escribir archivos arbitrarios.

Remediación / Referencias

Microsoft ya ha publicado actualizaciones para las tres vulnerabilidades englobadas bajo el nombre Proxyshell, aunque parte del problema radica en que no todos los administradores de servidores han realizado el parcheo correspondiente.

Por mayor información invitamos a visitar los siguientes sitios:
https://therecord.media/almost-2000-exchange-servers-hacked-using-proxyshell-exploit/
https://blog.segu-info.com.ar/2021/08/casi-2000-servidores-de-exchange.html

	**Dispositivos IoT son comprometidos por fallas de seguridad**	CRÍTICO

Descripción

Fuentes oficiales publican una falla de consideración crítica que afecta a millones de dispositivos IoT que utilizan la red ThroughTek "Kalay".

En publicaciones anteriores hemos explicado los problemas de seguridad que pueden presentar este tipo de dispositivos, muchos de tipo doméstico, que, al estar conectados a la red, son permeables a ser vulnerados pudiendo dejar expuesta información sensible de los usuarios.

Este error recientemente descubierto deja de manifiesto que los ciberdelincuentes pueden lograr interceptar la señal, comunicarse y controlar a los dispositivos inteligentes apuntados, llevando a cabo la ejecución código de forma remota.

Afectados

ThroughTek cuenta con más de 80 millones de dispositivos activos y más de 1.1 mil millones de conexiones mensuales en su plataforma. Dentro de sus clientes se pueden encontrar fabricantes de cámaras IoT, monitores inteligentes para bebés y productos de grabadora de video digital ("DVR").

"El protocolo Kalay se implementa como un kit de desarrollo de software ("SDK") que está integrado en el software del cliente (por ejemplo, una aplicación móvil o de escritorio) y en los dispositivos IoT en red, como las cámaras inteligentes. Debido a la forma en que los fabricantes de equipos originales ("OEM") y revendedores integran el protocolo Kalay antes de que los dispositivos lleguen a los consumidores, no se puede determinar una lista completa de productos y empresas afectadas por la vulnerabilidad descubierta."

Estado

La gravedad de esta falla radica en la posibilidad de que grupos delictivos accedan de forma remota a dispositivos IoT de los usuarios elegidos, vulnerando su privacidad mediante la escucha de audio en vivo, también ver datos de video en tiempo real y comprometer las credenciales del dispositivo y en algunos casos hasta poder tomar el control total a distancia sobre el dispositivo objetivo.

Remediación / Referencias

Si se tiene el SDK por debajo de la versión 3.1.10, se recomienda actualizar, además de tener habilitado Authkey y DTLS.

Por mayor información al respecto se puede acceder a:
https://blog.segu-info.com.ar/2021/08/vulnerabilidad-critica-afecta-millones.html

Adobe	Son detectadas vulnerabilidades en varios productos de Adobe	CRÍTICO

Descripción

Fuentes oficiales comparten información sobre errores críticos que afectan a diversos productos de Adobe y que están presentes en varias versiones. Se destaca que en caso de una explotación exitosa el atacante podría ejecutar código arbitrario en el sistema objetivo y comprometer información confidencial de los usuarios.

Afectados

- Adobe Photoshop 2020 versión 21.2.10 y anteriores.
- Adobe Photoshop 2021 versión 22.4.3 y anteriores.
- Adobe Bridge CC versión 11.1 y anteriores.
- Adobe Media Encoder: 15.0, 15.1, 15.2, 15.3, 15.4
- Adobe XMP-Toolkit-SDK 2020.1

Estado

No se ha detectado aun, una explotación activa sobre estos productos y versiones.

A continuación, el listado de los productos con las vulnerabilidades de mayor riesgo:

Photoshop: la falla permite a un atacante remoto ejecutar código arbitrario en el sistema objetivo. y comprometer el sistema.

Bridge: la falla permite a un atacante remoto ejecutar código arbitrario en el sistema objetivo. y comprometer el sistema objetivo.

Media Encoder: la falla permite a un atacante remoto comprometer el sistema objetivo.

XMP-Toolkit.SDK: la falla permite a un atacante remoto ganar acceso a información potencialmente sensible.

Remediación / Referencias

Se invita a realizar la instalación de las últimas actualizaciones disponibles por el proveedor para los productos y versiones afectados.

Por mayor información al respecto se puede acceder a:
https://www.csirt.gob.cl/vulnerabilidades/9vsa21-00482-01/
https://helpx.adobe.com/security/products/photoshop/apsb21-68.html
https://helpx.adobe.com/security/products/bridge/apsb21-69.htm
https://helpx.adobe.com/security/products/media-encoder/apsb21-70.html
https://helpx.adobe.com/security/products/xmpcore/apsb21-65.html

Microsoft	Se alerta por otro fallo detectado para #PrintNightmare	IMPORTANTE

Descripción

Especialistas alertan por una nueva vulnerabilidad que se suma al ya conocido error de cola de impresión en Windows (“PrintNightmare”), en este caso afectando otros componentes del sistema de impresión del sistema operativo en sus diferentes versiones.

“En este caso, la vulnerabilidad está relacionada con cómo se gestionan los archivos que cuentan con privilegios del sistema. Y es que, de nuevo, la falta de medidas de seguridad a la hora de ejecutar binarios supuestamente confiables en algún proceso relacionado con el sistema de impresión, es decir, lo que viene definiendo a PrintNightmare desde sus inicios, se puede traducir en la ejecución de código arbitrario, que comprometería la seguridad del sistema afectado.”

Afectados

PrintNightmare fue detectado con la publicación de Windows 365 y se estima que también pueda estar presente en la nueva versión de Windows 11.

Esto está pautado para el día 20 de octubre de 2021, por lo que se espera que, en un futuro cercano Microsoft pueda solucionar de manera permanente esta problemática de seguridad.

Estado

Este fallo posibilita que en caso de que se logre una explotación exitosa, los ciberdelincuentes podrían obtener ventajas sobre el SYSTEM mediante la elevación de privilegios.

De lo contrario a otras vulnerabilidades que componen este riesgo conocido como PrintNightmare, esta falla puntual es de ejecución local, disminuyendo su riesgo si se la compara con otras vulnerabilidades ya detectadas, debido a que no puede ser explotada remotamente.

"Es necesario que todo el ataque sea perpetrado y efectuado de manera local, en el sistema a atacar. Esto, sin duda, reduce los riesgos, pero no los erradica, y por ejemplo en un ataque en el que el atacante consiga desplazarse lateralmente hasta el servidor a atacar, o a un sistema de confianza del mismo, sí que podría llegar a armar un ataque."

Remediación / Referencias

Todavía no hay una solución formal, aunque el proveedor de tecnología expresa estar trabajando en ello. Se recomienda como remediación del problema, llevar a cabo la misma medida ya explicada en publicaciones anteriores respecto a otras amenazas de PrintNightmare.

Para protegerse de esta amenaza se deben deshabilitar las funciones de servidor de impresión en todos aquellos dispositivos en los que no se consideren tenerlo activo, en aquellos en los que sí, se deben revisar todas las políticas para reducir a lo imprescindible los permisos de ejecución de software por parte del sistema de impresión.

Por mayor información invitamos a visitar los siguientes sitios:
https://blog.segu-info.com.ar/2021/08/nueva-vulnerabilidad-publicada-de.html
https://www.muyseguridad.net/2021/08/17/printnightmare-otra-vulnerabilidad/

IISerpent: un malware que manipula el resultado de los navegadores

IMPORTANTE

Descripción

Especialistas alertan sobre un intento de fraude mediante un troyano que se ubica de lado del servidor y que tiene como objetivo alterar los resultados de búsqueda de los distintos navegadores de Internet, a través del secuestro de reputación de los sitios web que compromete.

"Nombramos al troyano IISerpent para destacar sus dos principales características: implementarse como una extensión maliciosa para el servidor web Internet Information Services (IIS) y utilizar técnicas para manipular los resultados de las páginas en los motores de búsqueda (SERP). Los operadores de IISerpent utilizan una variedad de técnicas de optimización para motores de búsqueda (SEO), en un intento por mejorar el posicionamiento de páginas de sitios web de terceros (probablemente sean los clientes que pagan a estos delincuentes)."

La técnica de Marketing Digital conocida como SEO refiere, a la búsqueda y rastreo que hacen los navegadores en Internet regularmente, para luego registrar todo el contenido que encontraron en línea, creando asociaciones entre los términos de búsqueda y el contenido, y utilizando varios algoritmos para determinar el posicionamiento de los resultados para términos de búsqueda específicos.

Este toryano conocido como IISerpent emplea técnicas de SEO no ético, ofreciendo "fraude de SEO como servicio", ya que emplea técnicas de SEO fraudulentas en servidores IIS vulnerados en beneficio de un tercero sin el consentimiento del webmaster.

Quienes llevan a cabo este tipo de fraude, utilizan este tipo de malware para mejorar el posicionamiento en los navegadores de búsqueda de las páginas de sitios web de terceros al hacer uso de la reputación del sitio web comprometido y emplear las siguientes técnicas:

- Redirigir a los motores de búsqueda al sitio web en particular elegido por el atacante, convirtiendo de manera efectiva al sitio web comprometido en una página de entrada.

- Inyectar una lista de backlinks (preconfigurados u obtenidos del servidor de C&C sobre la marcha) en la respuesta HTTP para los crawlers de motores de búsqueda, haciendo que los servidores comprometidos por IISerpent se conviertan en una especie de granja de enlaces

"Como consecuencia, el sitio web fraudulento puede aparecer mejor posicionado en los resultados que ofrecen los motores de búsqueda ya que es referenciado por sitios web de buena reputación, y esto repercute en la calificación del sitio."

Afectados

Se ha observado que los ataques de IISerpent, son dirigidas al servidor web IIS, en algunos casos utilizado para el ciberdelito y en otro para el ciberespionaje.

Estado

"IISerpent se implementa y configura como una extensión maliciosa para IIS, el software del servidor web de Microsoft. Eso permite al malware interceptar todas las solicitudes HTTP realizadas a los sitios web alojados por el servidor comprometido, pero también cambiar activamente las respuestas HTTP del servidor. Por ejemplo, robar información de las tarjetas de crédito utilizadas por clientes de sitios web de comercio electrónico (IIStealer) o para ejecutar comandos de backdoor en el servidor IIS comprometido (IISpy)."

Este tipo de troyano no afecta directamente al servidor comprometido ni a los usuarios del servidor, lo que hace IISerpent es escuchar y analiza todas las solicitudes HTTP enviadas al servidor comprometido, únicamente para buscar aquellas que se originan en crawlers de navegadores específicos.

Crawler: es un rastreador web, indexador web, indizador web o araña web es un programa informático que inspecciona las páginas del World Wide Web de forma metódica y automatizada.

Remediación / Referencias

Como medidas de precaución ante esta amenaza, recomendadnos mantener los servidores IIS actualizados y no realizar descargas de extensiones para IIS de fuentes que no sean confiables.

Por mayor información invitamos a visitar los siguientes sitios:
https://www.welivesecurity.com/la-es/2021/08/11/iiserpent-malware-para-realizar-fraude-seo-como-servicio/

Se publica el mayor DDoS jamás registrado

PREVENCIÓN

Descripción

Cloudflare es una empresa estadounidense de infraestructura web y seguridad de sitios web que proporciona servicios de mitigación de DDoS y redes de entrega de contenido. Recientemente informaron por parte de la organización, que han recibido el mayor ataque de denegación de servicio distribuido (DDoS) jamás registrado.

"Durante este ataque, Cloudflare afirma que recibió nada menos que 17,2 millones de peticiones HTTP por segundo (RPS). Para tener una perspectiva de cuán grande fue este ataque: Cloudflare atiende más de 25 millones de solicitudes HTTP por segundo en promedio. Esto se refiere a la tasa promedio de tráfico legítimo en el segundo trimestre de 2021. Por lo tanto, con un máximo de 17.2 millones de rps, este ataque alcanzó el 68% de nuestra tasa de rps promedio del segundo trimestre del tráfico HTTP legítimo."

Afectados

Se observó que el ataque proviene de la botnet Mirai y estaba dirigido un cliente de Cloudflare perteneciente a la industria financiera. La red de bots de Mirai envió más de 330 millones de solicitudes de ataque dirigidos.

El promedio de peticiones legítimas que recibe Clouflare es de 25 millones por segundo, representando este ataque un 68% de peticiones malintencionadas del promedio de solicitudes legítimas que recibe normalmente.

"El tráfico de ataques se originó en más de 20.000 bots en 125 países de todo el mundo. Según las direcciones IP de origen de los bots, casi el 15% del ataque se originó en Indonesia y otro 17% en India y Brasil combinados. Indica que puede haber muchos dispositivos infectados con malware en esos países."

Vector de Ataque

Los especialistas creen que la gran mayoría de esto ataques provienen de la botnet Mirai, la cual es responsable de causar algunos de los mayores ataques DDoS registrados.

"Mirai se propaga infectando dispositivos operados por Linux, como cámaras de seguridad y routers. Luego, se autopropaga buscando los puertos Telnet abiertos 23 y 2323. Una vez encontrados, intenta obtener acceso a dispositivos vulnerables mediante la fuerza bruta de credenciales conocidas, como nombres de usuario y contraseñas predeterminados de fábrica. Las variantes posteriores de Mirai también aprovecharon las vulnerabilidades Zero-Day en routers y otros dispositivos. Una vez infectados, los dispositivos monitorearán un servidor de Command&Control (C2) para obtener instrucciones sobre qué objetivo atacar."

Remediación / Referencias

Por mayor información al respecto se puede acceder a:
https://blog.segu-info.com.ar/2021/08/reportado-ataque-ddos-de-mas-de-172m.html
https://blog.cloudflare.com/cloudflare-thwarts-17-2m-rps-ddos-attack-the-largest-ever-reported/

Conclusiones

Seguimos viendo la importancia de estar atentos a las nuevas amenazas emergentes, 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.

Además, alertamos a estar prevenidos en cuanto al Phishing, ya que se observa un incremento de este tipo de técnica fraudulentas. En este caso destacamos la presencia de IISerpent un malware que manipula el resultado de los navegadores, por lo que recomendadnos mantener los servidores IIS actualizados y no realizar descargas de extensiones para IIS de fuentes que no sean confiables.

Finalmente, debido a las fallas que siguen apareciendo para el ya conocido error de cola de impresión en Windows (“PrintNightmare”), recomendamos prestar principal atención en deshabilitar las funciones de servidor de impresión en todos aquellos dispositivos en los que no se consideren tenerlo activo, en aquellos en los que sí, se deben revisar todas las políticas para reducir a lo imprescindible los permisos de ejecución de software por parte del sistema de impresión.

Datasec queda a su entera disposición, en caso de consultas invitamos a comunicarse a:
soc@datasec-soft.com