



Boletín de Ciberseguridad

Fecha de Publicación
25/04/2021 - N.º 6

Mes de Abril
11/04/2021 - 25/04/2021

Índice

Introducción	pág. 2
Fallas en VMWare ESXi son explotadas por RansomExx.....	pág. 3
Dispositivos IoT presentan vulnerabilidades de consideración.....	pág. 4
Ejecución de código remoto en Buscadores Chrome, Edge, Opera y Brave	pág. 6
Malware utiliza LinkedIn para realizar Fraude.....	pág. 7
Páginas Web con PDF maliciosos para realizar Fraude.....	pág. 8
Actualizaciones disponibles para errores críticos en Microsoft Exchange.....	pág. 10
Conclusiones.....	pág. 12

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 abril 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:

Fallas en VMWare ESXi son explotadas por RansomExx

“Al menos dos bandas importantes de ransomware están abusando de las vulnerabilidades del producto VMWare ESXi para tomar el control de máquinas virtuales implementadas en entornos empresariales y cifrar sus discos duros virtuales.”

Malware utiliza LinkedIn para realizar Fraude

“Una nueva campaña de spear-phishing está dirigida a profesionales en LinkedIn con ofertas de trabajo, armadas en un intento de infectar objetivos con un sofisticado troyano de puerta trasera en JScript llamado "more_eggs".”

Actualizaciones disponibles para errores críticos en Microsoft Exchange

“En este mes de abril de 2021 de Microsoft corrigió 108 fallas y 5 Zero-Days. Han sido unos meses difíciles para los administradores de Windows y Microsoft Exchange, y parece que abril no será más fácil.”



Fallas en VMWare ESXi son explotadas por RansomExx

CRÍTICO

Descripción

Recientemente ha sido descubierto un ransomware que se aprovecha de errores críticos en VMWare ESXi, tomando el control de equipos virtuales usados en distintas organizaciones.

“Las vulnerabilidades permiten a un atacante en la misma red enviar solicitudes SLP maliciosas a un dispositivo ESXi y tomar el control de él, incluso si el atacante no ha logrado comprometer el servidor VMWare vCenter al que suelen informar las instancias ESXi.”

Esto provoca que se den cortes masivos perjudicando la operatividad diaria de la organización atacada, debido a que los discos virtuales ESXi comúnmente son utilizados para centralizar información de otros sistemas.

Afectados

Producto Afectado: VMWare ESXi

“VMware ESXi (anteriormente VMware ESX) es un programa de virtualización a nivel de centro de datos producido por VMware, Inc.. Es el componente de su producto VMware Infraestructure que se encuentra al nivel inferior de la capa de virtualización, el hipervisor, aunque posee herramientas y servicios de gestión autónomos e independientes.”

Estado

Se piensa que el ataque ha sido efectuado por el grupo criminal que diseñó el ransomware RansomExx, y que está siendo explotado por otras dos bandas criminales.

La explotación apunta a Service Location Protocol (SLP)

“El protocolo de ubicación de servicios (SLP) es un protocolo de la Internet Engineering Task Force (IETF) para descubrir recursos compartidos (como impresoras, servidores de archivos, netcams, etc.) en una red de empresa. El sistema operativo Solaris 8 contiene una implementación total de SLP que incluye API que permiten a los desarrolladores escribir aplicaciones habilitadas para SLP y proporciona a los administradores de sistemas una estructura que facilita la ampliación de la red.”

Se está seguro que ha sido puesto a la venta el acceso a instancias de ESXi en la DeepWeb.

Remediación / Referencias

Recomendamos a aquellos usuarios de VMWare ESXi buscar las actualizaciones para ESXi o en todo caso deshabilitar el protocolo SLP para evitar los ataques, si el protocolo no es necesario.

Por mayor información acceder a:

<https://blog.segu-info.com.ar/2021/04/ransomware-apunta-vulnerabilidades-de.html>

<https://www.zdnet.com/article/ransomware-gangs-are-abusing-vmware-esxi-exploits-to-encrypt-virtual-hard-disks/>



Dispositivos IoT presentan vulnerabilidades de consideración

IMPORTANTE

Descripción

Se confirmó un conjunto de vulnerabilidades que perjudican los DNS. Se trata de unos nueve errores en pilas de comunicación de red TCP/IP. Estos son utilizados por millones de equipos IoT con sistemas operativos de código abierto u Open Source.

NAME:WRECK es el nombre elegido para denominar a estas fallas. Si se llevara a cabo un exploit exitoso el atacante podría obtener control sobre el equipo vulnerado pudiendo desconectarlos dejándolos sin operatividad.

“Podrían obtener datos confidenciales, modificar el funcionamiento o incluso hacer que no puedan estar disponibles.”

“Si observamos las nueve vulnerabilidades descubiertas, la puntuación de gravedad oscila entre 5,3 y 9,8.”

Afectados

Dentro de los productos afectados podemos destacar servidores de alto rendimiento o equipos de Red.

Afecta a varias pilas TCP/IP muy usadas como son las siguientes:

FreeBSD - Versión vulnerable 12.1: Se trata de uno de los sistemas operativos más populares de la familia BSD.

IPnet - Versión vulnerable VxWorks 6.6: Desarrollado inicialmente por Interpeak, ahora está bajo mantenimiento de WindRiver y utilizado por el sistema operativo de VxWorks.

NetX - Versión vulnerable 6.0.1: Forma parte de ThreadX RTOS y ahora es un proyecto de código abierto mantenido por Microsoft bajo el nombre Azure RTOS NetX.

Nucleus NET - Versión vulnerable 4.3: Parte de Nucleus RTOS mantenido por Mentor Graphics, una empresa de Siemens, se utiliza en dispositivos médicos, industriales, de consumo, aeroespacial y del Internet de las cosas.

Estado

“Un atacante podría explotar cualquiera de estas vulnerabilidades de NAME:WRECK y tener como objetivo atacar a servidores empresariales o gubernamentales, instalaciones en hospitales y otras muchas organizaciones de menor tamaño. “

Todas las vulnerabilidades detectadas pueden ser explotables, aunque no todos tienen el mismo impacto. Aquellos errores más graves que pueden suponer la ejecución remota de código, han obtenido una puntuación de gravedad de 9,8 sobre 10.

Remediación / Referencias

Las actualizaciones para estos errores NAME:WRECK ya están disponibles para FreeBSD, Nucleus NET y NetX, y es posible eliminar los problemas si las correcciones llegan a los productos afectados.


“El informe de Forescout profundiza en los detalles técnicos sobre cómo la explotación puede conducir a un ataque de ejecución de código remoto exitoso al aprovechar varias de las vulnerabilidades de NAME:WRECK, así como errores de la colección AMNESIA:33, que la compañía descubrió en la Pila TCP/IP de código abierto. Pilas de IP.”

También existen dos herramientas de código abierto que pueden ayudar a determinar si un dispositivo de red ejecuta una pila TCP/IP específica: Project Memoria Detector - Joern Scan.

Por mayor información invitamos a visitar los siguientes sitios:

<https://blog.segu-info.com.ar/2021/04/vulnerabilidades-namewreck-afecta.html>

<https://www.bleepingcomputer.com/news/security/name-wreck-dns-vulnerabilities-affect-over-100-million-devices/>

	Ejecución de código remoto en Buscadores Chrome, Edge, Opera y Brave	IMPORTANTE
--	---	-------------------

Descripción

Ha sido publicada la explotación de una falla en el motor de renderizado de JavaScript V8 de Chromium, en el que se basan los buscadores web Chrome, Microsoft Edge, Opera y Brave. Mediante esta vulnerabilidad un atacante podría realizar una ejecución de código remoto (RCE)

RCE: El término ejecución arbitraria de código (del inglés arbitrary code execution) hace referencia, en el campo de la seguridad informática, a la capacidad de un atacante para ejecutar comandos o inyectar código en una aplicación a su antojo, aprovechando generalmente alguna vulnerabilidad (por ejemplo, un desbordamiento de búfer).

Afectados

Buscadores Chrome, Edge, Opera y Brave, los cuales cuentan con más de 900 millones de usuarios.

Estado

La explotación funciona en cualquier navegador basado en Chromium (sin actualizar) y en cualquier sistema operativo.

Actualmente hay un exploit activo sobre estos buscadores, perpetuados por diferentes grupos delictivos.

Remediación / Referencias

Google ha abordado el problema en la última versión de V8 y, si bien se espera que Google publique Chrome 90, mientras tanto es importante actualizar a Chromium 89.0.4389.128 en cualquier navegador.

Por mayor información invitamos a visitar los siguientes sitios:

<https://blog.segu-info.com.ar/2021/04/zero-day-para-vulnerabilidad-rce-en.html>

<https://thehackernews.com/2021/04/rce-exploit-released-for-unpatched.html>

**Linked in****Malware utiliza LinkedIn para realizar Fraude****IMPORTANTE****Descripción**

Una nueva campaña de spear-phishing está dirigida a profesionales en LinkedIn con ofertas de trabajo, armadas en un intento de infectar objetivos con un sofisticado troyano backdoor en JScript llamado "more_eggs".

Backdoor: Es un Tipo de troyano que permite el acceso al sistema infectado y su control remoto. El atacante puede entonces eliminar o modificar archivos, ejecutar programas, enviar correos masivamente o instalar herramientas maliciosas.

Spear-Phishing: El spear phishing es una estafa de correo electrónico o comunicaciones dirigida a personas, organizaciones o empresas específicas. Aunque su objetivo a menudo es robar datos para fines maliciosos, los cibercriminales también pueden tratar de instalar malware en la computadora de la víctima.

“Una vez instalado, more_eggs mantiene un perfil sigiloso al secuestrar procesos legítimos de Windows mientras presenta un documento señuelo "solicitud de empleo" para distraer a los objetivos de las tareas en segundo plano en curso desencadenadas por el malware. ”

Afectados

Usuarios de LinkedIn.

“LinkedIn tiene 675 millones de usuarios mensuales, y gana dos nuevos miembros cada segundo. El 12 % de la población mundial (mayor a 13 años) está en LinkedIn.”

Estado

“Para aumentar las probabilidades de éxito, los señuelos de phishing aprovechan los archivos ZIP maliciosos que tienen el mismo nombre que el de los puestos de trabajo de las víctimas, tomados de sus perfiles de LinkedIn. Por ejemplo, si el trabajo del miembro de LinkedIn aparece como "Ejecutivo de cuentas sénior", el archivo ZIP malicioso se llamaría igual.”

Cuando la victima abre la oferta de trabajo fraudulenta, se instala en el equipo del usuario el troyano more_eggs.

Hasta el momento no se sabe con exactitud quien está llevando a cabo este exploit, aunque se sabe que con anterioridad, el JScript de more_eggs fue implementado por grupos de cibercriminales conocidos como Cobalt, FIN6 y EvilNum

Remediación / Referencias

Se invita a difundir esta noticia a quienes usen LinkedIn, además de estar prevenidos y atentos a nuevos modos de implementación de Fraudes activos.

Por mayor información al respecto se puede acceder a:

<https://blog.segu-info.com.ar/2021/04/falsas-ofertas-de-trabajo-en-linkedin.html>

<https://thehackernews.com/2021/04/hackers-targeting-professionals-with.html>



Páginas Web con PDF maliciosos para realizar Fraude

IMPORTANTE

Descripción

Cuando hablamos de formatos de archivo de PDF se destaca su formato, utilidad y funcionamiento, siendo ampliamente utilizado tanto en entornos educativos como empresariales. El problema radica en las descargas de este tipo de archivos y el lugar de origen. Ya que podrían contener metadatos y cargar con malwares u otro tipo de información maliciosa con el fin de infectar los equipos de los usuarios.

Este problema no es propio solamente de PDF, si no que otros archivos de OpenOffice pueden presentar el mismo riesgo si no se esta atento de como buscar y gestionar los archivos que vamos a descargar.

“En este caso se ha descubierto una técnica que consiste en crear páginas web de recursos profesionales útiles (plantillas de facturas, de presupuestos, escritos, etcétera) con los PDF, con la intención de que los usuarios creen que dichas páginas son fiables, así como su contenido, y los descarguen y abran, infectando así sus ordenadores.”

Afectados

Los cibercriminales han puesto en circulación cientos de miles de sitios web con PDF maliciosos utilizando Google Sites.

Google Sites: es una aplicación en línea gratuita ofrecida por la empresa estadounidense Google como parte de la suite de productividad de G Suite. Es una herramienta para la creación de páginas web. Esta aplicación permite crear un sitio web o una intranet de una forma tan sencilla como editar un sitio web.

Estos sitios creados de manera malintencionada utilizan palabras claves populares, como factura, estado de cuenta, recibo, cuestionario, de esa manera cuando un usuario busca en el navegador una plantilla comercial específica, está la posibilidad de que en los resultados principales de la búsqueda estén las direcciones a estos sitios con PDF infectados.

Estado

“El proceso de infección se basa en explotar al usuario, no a una aplicación. El usuario simplemente ejecuta un binario disfrazado de PDF para infectar la máquina. Esta es una tendencia cada vez más común con la entrega de malware, que habla de la seguridad mejorada de aplicaciones como los navegadores que manejan código vulnerable. Desafortunadamente, revela un punto ciego evidente en los controles que permiten a los usuarios ejecutar binarios o archivos de script que no son de confianza a voluntad.”

Una vez descargados y abiertos, los PDF de estas páginas proceden a instalar una RAT (Remote Access Tool) con la que hacerse con el control del sistema, que podrán emplear posteriormente con tantos fines como deseen. Adicionalmente, pueden emplear esta herramienta para garantizarse un acceso persistente al sistema incluso si la RAT es eliminada del mismo.

Remediación / Referencias

Es importante comprobar el origen y confiabilidad de las paginas que visitamos y los archivos que descargamos en nuestros equipos, por eso hay que estar prevenidos y atentos a nuevas estrategias que utilizan los ciberdelincuentes para vulnerar nuestra seguridad.

Por mayor información al respecto se puede acceder a:

<https://blog.segu-info.com.ar/2021/04/crean-100000-paginas-web-con-pdf.html>

<https://www.muysseguridad.net/2021/04/15/100000-paginas-con-pdf-maliciosos/>



Actualizaciones disponibles para errores críticos en Microsoft Exchange

PREVENCIÓN

Descripción

En este mes de abril de 2021 de Microsoft corrigió 108 fallas y 5 Zero-Days. Han sido unos meses difíciles para los administradores de Windows y Microsoft Exchange, y parece que abril no será más fácil.

“Con la actualización de hoy, Microsoft ha corregido 108 vulnerabilidades, 19 clasificadas como críticas y 89 como importantes. Estos números no incluyen las 6 vulnerabilidades de Chromium Edge lanzadas a principios de este mes.”

Afectados

Windows - Microsoft Exchange

Vulnerabilidades: Escalamiento de privilegios del servicio RPC Endpoint Mapper.
Escalamiento de privilegios de biblioteca ms-rest-nodeauth de Azure.
Escalamiento de privilegios de Win32k explotada activamente.
Divulgación de información del instalador de Windows: PolarBear.
Denegación de servicio de Windows NTFS.

Vector de Ataque

Microsoft Exchange Server RCE

Se cree que una de las fallas más graves está siendo aprovechada por varios grupos delictivos. El error consiste en un escalamiento de privilegios (EoP) y es utilizado junto a otros exploits para escapar de la Sandbox y obtener privilegios en el sistema operativo.

Sandbox: En seguridad informática, el aislamiento de procesos o entorno aislado es un mecanismo para ejecutar programas con seguridad y de manera separada. A menudo se utiliza para ejecutar código nuevo, o software de dudosa confiabilidad proveniente de terceros

“Otra de ella es una vulnerabilidad de escritura fuera de los límites (OOB) en el archivo dwmcore.dll, que forma parte de Desktop Window Manager (dwm.exe). DirectComposition es un componente de Windows que se introdujo en Windows 8 para permitir la composición de mapas de bits con transformaciones, efectos y animaciones, con soporte para mapas de bits de diferentes fuentes (GDI, DirectX, etc.).”

Remediación / Referencias

Para obtener información sobre las actualizaciones de Windows se puede leer acerca de las actualizaciones acumulativas de Windows 10 KB5001330 y KB5001337.

Por mayor información al respecto se puede acceder a:

<https://support.microsoft.com/es-es/windows/actualizar-windows-10-3c5ae7fc-9fb6-9af1-1984-b5e0412c556a>

<https://blog.segu-info.com.ar/2021/04/parches-de-abril-exploit-activo-en.html>

<https://www.bleepingcomputer.com/news/microsoft/microsoft-april-2021-patch-tuesday-fixes-108-flaws-5-zero-days/>

Conclusiones

La tendencia de crecimiento en ataques relacionados a la extorsión de datos (Malware tipo Ransomware) han venido en aumento desde el año 2020 y en este año y muy probablemente también relacionado a los ámbitos de teletrabajo, es que el ransomware evolucionó, haciéndose más efectivo.

Durante 2020, las bandas que operan las distintas familias de ransomware dejaron atrás las campañas masivas y al azar esperando que alguna víctima se infecte y que eventualmente pague el rescate para recuperar su información. En cambio, apuntaron a compañías de varias industrias, así como al sector de la salud y a organismos gubernamentales a nivel global, llevando adelante ataques en los que secuestran mediante cifrado los archivos en los equipos comprometidos, con nuevas estrategias para demandar el pago de un rescate.

El robo de información previo al cifrado de los archivos y la posterior extorsión bajo la amenaza de publicar, vender o subastar los datos confidenciales robados fue una metodología que se observó por primera vez a fines de 2019 y que se consolidó en 2020. El objetivo es agregar un plan B a la estrategia de sólo cifrar los archivos y demandar el pago de un rescate para devolver el acceso. Con este nuevo método, adoptado ya por varias familias de ransomware, los criminales aumentan la posibilidad de monetizar los ataques al contar con otro instrumento para presionar a las víctimas y que se decidan a pagar, ya que supuestamente de esta manera evitarán la divulgación de la información robada y recuperarán el acceso a los datos.

El robo de información sensible previo al cifrado para luego extorsionar a la víctima con la filtración de información fue, por ejemplo, una práctica que se vio por primera vez con el ransomware Maze a finales de 2019, pero inspiró a otros grupos de ransomware que adoptaron esta estrategia temprano en 2020, como fue el caso de Sodinokibi, DoppelPaymer, RobinHood o Nemty. Hoy en día, la gran mayoría de estas bandas cuenta con un sitio web en el que publican los nombres de sus nuevas víctimas y filtran la información robada en caso de que la víctima no quiera pagar el rescate. Pero además de esta práctica extorsiva, otros como Suncrypt o Avaddon (una familia muy activa en lo que va de 2021) comenzaron también a implementar los ataques de DDoS a los sitios de sus víctimas para convencerlos de la necesidad de pagar.

En cuanto a los sectores a los que más han apuntado y han estado afectados de estos ataques son tanto de tecnología, organismos gubernamentales e infraestructuras críticas han sido los principales blancos, seguidos por el sector de la salud, transporte, manufactura, servicios financieros y educación.

Uno de los ataques de ransomware más importantes a nivel global se registró en septiembre de 2020 y estuvo dirigido a la Universal Health Services, una de las cadenas de hospitales más grandes de los Estados Unidos. El ataque del ransomware Ryuk afectó a cientos de sus sedes e interrumpió el funcionamiento de los sistemas informáticos, servicios telefónicos, Internet y los data centers. Según NBC, fue probablemente el ciberataque al sector de la salud más grande en la historia de los Estados Unidos.

La rentabilidad del modelo del ransomware-as-a-service junto con el incremento del valor del bitcoin son un gran atractivo para criminales sin conocimientos técnicos que ven en estos modelos la oportunidad de obtener ganancias financieras.

El aumento de los ataques dirigidos de ransomware también tiene una explicación por el uso de este modelo (RaaS), donde algunos actores desarrollan estos códigos maliciosos y los ofrecen en la dark web para asociarse con afiliados que se encargarán de la distribución del ransomware y luego dividirán las ganancias. Estas familias de ransomware muchas veces operan durante algún tiempo y cesan sus actividades, dando lugar a la creación de otros grupos de ransomware que adquieren el código fuente y le añaden en algunos casos variaciones.

La importancia de una correcta segmentación de ambientes, datos y permisos de usuarios acotados, sumado a la gestión continua de vulnerabilidades son las protecciones mínimas que tenemos que contar en nuestras organizaciones para protegernos de estos escenarios.