Boletín de Ciberseguridad

Fecha de Publicación
02/08/2021 - N.º 13

Mes de Agosto
19/07/2021 - 02/08/2021

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 primera quincena del mes de agosto se destacan 8 noticias de relevancia: 4 sobre vulnerabilidades tecnológicas, 1 de fraude activos y 3 de prevención.

Aquellas noticias a tener especial recaudo son las siguientes:

Windows es afectado por Prueba de Concepto publicada en GitHub
Ha sido expuesta una vulnerabilidad en Windows que, en el caso de ser explotada, puede dirigir a los equipos de los usuarios para que de manera remota se autentiquen y compartan sus hashes de contraseña con los ciberdelincuentes.

Vulnerabilidad de Escalamiento de Privilegios Locales (LPE) en Linux
Esta vulnerabilidad se ha denominado como “Sequoia” y se identifica en la capa del sistema de archivos utilizada para administrar los datos del usuario, una característica utilizada universalmente por todos los principales sistemas operativos Linux.

Alerta sobre error que permite elevación de privilegios en Windows
Especialistas en ciberseguridad advierten sobre una vulnerabilidad presente en Windows en Windows 10/11 que permite Escalamiento de Privilegios Locales (LPE).

Aviso sobre Zero-day corregidos en iOS, iPadOS y macOS
Apple publicó actualizaciones para una vulnerabilidad que está presente en varios de sus sistemas operativos, como iOS, iPadOS y macOS. Es una vulnerabilidad del tipo zero-day que está siendo explotada en la actualidad.

Microsoft	**Windows es afectado por Prueba de Concepto publicada en GitHub**	CRÍTICO

Descripción

Ha sido expuesta una vulnerabilidad en Windows que, en el caso de ser explotada, puede dirigir a los equipos de los usuarios para que de manera remota se autentiquen y compartan sus hashes de contraseña con los ciberdelincuentes.

Se trata de una de prueba de concepto (PoC) publicada recientemente en GitHub que recibió el nombre de Petipotam.

Si el ataque fuera exitoso podría permitir a un atacante ejecutar código de forma remota en una máquina con Windows o moverse lateralmente en la red a sistemas críticos como servidores que alojan controladores de dominio.

Afectados

Especialistas en ciberseguridad consideran que este ataque afecta a la mayoría de las versiones de Windows compatibles en la actualidad. De igual manera se destaca que los sistemas Windows 10, Windows Server 2016 y Windows Server 2019, son los más afectados.

Estado

Se trata de un ataque de retransmisión (relay) NTLM. Windows ha mantenido NTLM debido a la compatibilidad con sistemas y aplicaciones de versiones anteriores, agregando complejidad y debilidad a las implementaciones de Active Directory en particular.

NTLM: En una red de Windows, NT LAN Manager es un conjunto de protocolos de seguridad de Microsoft destinados a proporcionar autenticación, integridad y confidencialidad a los usuarios.

"En un ataque de retransmisión (relay) NTLM, un atacante establece una posición entre el cliente y el servidor en la red e intercepta el tráfico de autenticación. Las solicitudes de autenticación del cliente son enviadas al servidor por el atacante, de manera similar, los desafíos se transmiten al cliente y las respuestas de autenticación válidas al desafío del cliente se envían de vuelta al servidor, lo que permite al atacante, en lugar del cliente, autenticarse utilizando los datos y credenciales del cliente."

Remediación / Referencias

Es muy importante validar y monitorear Kerberos y Active Directory para prevenir otro tipo de ataques.

"La única forma de mitigar esta técnica es deshabilitar la autenticación de NTLM o permitir protecciones, como la firma de SMB, la firma de LDAP y la unión de canales."

Por mayor información acceder a:
https://blog.segu-info.com.ar/2021/07/nuevo-ataque-petitpotam-obliga-windows.html
https://www.bleepingcomputer.com/news/microsoft/new-petitpotam-attack-allows-take-over-of-windows-domains/

Linux	Vulnerabilidad de Escalamiento de Privilegios Locales (LPE) en Linux	CRÍTICO

Descripción

Esta vulnerabilidad se ha denominado como "Sequoia" y se identifica en la capa del sistema de archivos utilizada para administrar los datos del usuario, una característica utilizada universalmente por todos los principales sistemas operativos Linux.

Los atacantes sin privilegios pueden obtener privilegios de root al explotar una vulnerabilidad de Escalamiento de Privilegios Locales (LPE) en las configuraciones predeterminadas de la mayoría de las distribuciones de Linux.

Afectados
Esta falla afecta a todas las versiones del kernel de Linux lanzadas desde 2014.

Estado
"Una vez explotado con éxito en un sistema vulnerable, los atacantes obtienen privilegios de root completos en instalaciones predeterminadas de muchas distribuciones modernas. "

También se advierte de la existencia de un error que puede ser explotado por atacantes sin privilegios, provocando una denegación de servicio por agotamiento de la pila identificada en systemd.

Remediación / Referencias
Como este ataque afecta muchas distribuciones y versiones de Linux, se recomienda a los usuarios que instalen las actualizaciones correspondientes ofrecidas por el proveedor.

Por mayor información invitamos a visitar los siguientes sitios:
https://blog.segu-info.com.ar/2021/07/nuevo-bug-del-kernel-de-linux-permite.html

iPhone	**Falla en WiFi perjudica a equipos Iphone**	IMPORTANTE

Descripción
Recientemente fue publicada una falla que bloqueaba el servicio Wifi en iPhones que, en caso de ser vulnerada por un atacante, puede resultar en la ejecución código de forma remota sin la interacción del usuario.

Cuando se reveló inicialmente, el error podría deshabilitar la conexión WiFi de un iPhone después de intentar conectarse a una red con un nombre (SSID) que incluye un carácter especial.

Arreglar el error fue tan simple como restablecer la configuración de red para eliminar los nombres de todas las redes WiFi, incluida la maliciosa, de las listas de SSID conocidos a los que podría unirse.

Los investigadores demostraron que hay más en este error que la condición de denegación de servicio (DoS) de WiFi reportada inicialmente.

Afectados
Las evidencias demuestran que esta falla es explotable en iOS 14 a 14.4 y iOS 14.6 cuando se conecta a un SSID creada de forma malintencionada.

Estado

Este ataque fue denominado como WiFiDemon y es importante destacar que el error se puede desencadenar como un Zero-Click (sin interacción del usuario) y tiene potencial para la ejecución remota de código. Se puede considerar que este problema es similar a un error de cadenas de formato, donde la computadora ve el valor de entrada como un carácter de formato, no como un carácter.

Un escenario que puede llevar a la ejecución de código en el dispositivo de destino es crear una red WiFi maliciosa y esperar a que la víctima se conecte.

"En versiones anteriores de iOS, incluso si la víctima no se une a la red maliciosa, el servicio WiFi se bloquea y se reinicia en un bucle inmediatamente después de leer el nombre SSID mal elaborado. Si el error se explota localmente, podría ayudar a un atacante a construir una sand-box para poder hacer jailbreak al dispositivo."

Remediación / Referencias

Se recomienda actualizar los dispositivos utilizados con la última versión del sistema operativo. También es importante deshabilitar la función de unión automática en la configuración de WiFi, que protege al usuario contra ataques de inundación de puntos de acceso.

Ya están disponible las actualizaciones de seguridad de iOS 14.7 de Apple.

Por mayor información invitamos a visitar los siguientes sitios:
https://blog.segu-info.com.ar/2021/07/vulnerabilidad-de-wifi-de-iphone-se.html
https://www.bleepingcomputer.com/news/apple/iphone-wifi-bug-morphs-into-zero-click-hacking-but-theres-a-fix/amp/

	**Fue publicada vulnerabilidad detectada en Apple**	IMPORTANTE

Descripción

Fuentes oficiales informan de una vulnerabilidad detectada en productos Apple que está siendo explotada de manera activa en la actualidad.

La vulnerabilidad corresponde a un error de desbordamiento de buffer, que permite escalar privilegios en el sistema afectado. Una aplicación local puede detonar corrupción de memoria y ejecutar código arbitrario en el sistema objetivo.

Afectados

- macOS: 11.0 20A2411 a 11.5 20G71.
- iPadOS: 14.0 18A373 a 14.7 18G70.
- Apple iOS: 14.0 18A373 al 14.7 18G69.

Estado

Desbordamiento de Buffer: "Un desbordamiento de búfer es un error de software que se produce cuando un programa no controla adecuadamente la cantidad de datos que se copian sobre un área de memoria reservada a tal efecto (buffer): Si dicha cantidad es superior a la capacidad preasignada, los bytes sobrantes se almacenan en zonas de memoria adyacentes, sobrescribiendo su contenido original, que probablemente pertenecían a datos o código almacenados en memoria. Esto constituye un fallo de programación."

Remediación / Referencias

Para mitigar esta vulnerabilidad recomendamos instalar las respectivas actualizaciones entregadas por el proveedor.

Por mayor información invitamos a visitar los siguientes sitios:
https://support.apple.com/en-us/HT212622
https://support.apple.com/en-us/HT212623
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30807

OneDrive	**Intento de robo de credenciales mediante sitio web fraudulento**	IMPORTANTE

Descripción

Fuentes oficiales advierten de un intento de robo de credenciales de usuarios, mediante la existencia de un sitio web fraudulento que tiene como motivo remplazar a la página oficial de Microsoft OneDrive.

En el caso que este intento de phishing resulte exitoso, puede afectar a usuarios, clientes y a la imagen institucional de la organización aludida.

Afectados

Servicio de Cloud OneDrive, las características que pueden ser afectadas:

- Office 365Online.
- Uso compartido de favoritos.
- Integración con Grupos.
- RSS Feeds.
- Descargas de archivos. zip.
- Gestión de Fotos e Imágenes.
- App.

Estado

Indicadores de compromiso
URL sitio falso: https://lomasdequillon[.]cl/879898iikblinfdteere/spider/error.html
Certificado Digital
Fecha Válido: 28-01-2021
Fecha Término:28-04-2021
Emitido: Let's Encrypt R3

Datos Alojamiento
IP: [50.87.153.17]
Número de Sistema Autónomo (AS):46606
Etiqueta del Sistema Autónomo UNIFIEDLAYER-AS-1
País: US
Registrador: ARIN

Datos del Dominio
Nombre de Dominio lomasdequillon[.]cl
Creado: 23-01-2008
Expira: 18-02-2024
Información del Registrador: nic.cl
Correo Electrónico: abuse@nic.cl
Name Server: ns4012.websitewelcome.com
ns4011.websitewelcome.com

Remediación / Referencias

- 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://www.csirt.gob.cl/alertas/8ffr21-00912-01/

FORTINET	**Falla descubierta en Fortinet permite ejecutar código como Administrador**	PREVENCIÓN

Descripción

Actualizaciones de seguridad fueron publicadas recientemente por Fortinet sobre una falla grave que afectaba a las soluciones de administración de red FortiManager y FortiAnalyzer. Estos parches mitigan un error que permitía a usuarios no autenticados ejecutar código de forma remota como Administrador.

Afectados

- FortiManager versiones 5.6.10 y anteriores.
- FortiManager versiones 6.0.10 y anteriores.
- FortiManager versiones 6.2.7 y anteriores.
- FortiManager versiones 6.4.5 y anteriores.
- FortiManager versión 7.0.0.
- Versiones de FortiManager 5.4.x.
- FortiAnalyzer versiones 5.6.10 y anteriores.
- FortiAnalyzer versiones 6.0.10 y anteriores.
- FortiAnalyzer versiones 6.2.7 y anteriores.
- FortiAnalyzer versiones 6.4.5 y anteriores.
- FortiAnalyzer versión 7.0.0.

Vector de Ataque

"La vulnerabilidad es un problema del tipo Use After Free que un atacante podría aprovechar para ejecutar código arbitrario como root mediante el envío de una solicitud específicamente diseñada al servicio "fgfmsd daemon" del dispositivo objetivo".

"Un atacante podría desencadenar la falla enviando una solicitud especialmente diseñada al puerto "FGFM" de un dispositivo vulnerable, el cual está deshabilitado de forma predeterminada en FortiAnalyzer y solo se puede habilitar en modelos de hardware específicos, incluidos 1000D, 1000E, 2000E, 3000D, 3000E, 3000F, 3500E, 3500F, 3700F, 3900E."

Este error ha recibido una puntuación CVSS general de 7.7, debido a la alta posibilidad de realizar ataques dirigidos. No hay indicios de que esta falla se esté explotando activamente en la naturaleza.

Remediación / Referencias

Una forma de mitigar esta vulnerabilidad consiste en deshabilitar las funciones de FortiManager en la unidad FortiAnalyzer mediante las siguientes instrucciones:

comando: config system global
set fmg-status disable (por defecto está disabled)
end

Por mayor información al respecto se puede acceder a:
https://blog.segu-info.com.ar/2021/07/fortinet-corrige-un-error-que-permite.html
https://www.theregister.com/2021/07/20/fortinet_rce/

	**Aviso sobre Zero-day corregidos en iOS, iPadOS y macOS**	PREVENCIÓN

Descripción

Apple publicó actualizaciones para una vulnerabilidad que está presente en varios de sus sistemas operativos, como iOS, iPadOS y macOS. Es una vulnerabilidad del tipo zero-day que está siendo explotada en la actualidad.

En enero de 2021 Apple ya había mitigado tres fallas zero-day en iOS, en mayo parcheó otras cuatro zero-day que afectaban a dispositivos iPhone, macOS, iPads, iPods y Apple Watch. En el mes de mayo corrigió una zero-day en macOS y en junio otras dos en iOS

Afectados

- iOS,
- iPadOS
- macOS

Vector de Ataque

"Se trata de un fallo de corrupción de memoria en la extensión de kernel IOMobileFramebuffer que permite ejecutar en código arbitrario con privilegios de kernel un dispositivo vulnerable."

Remediación / Referencias

Los parches publicados por el proveedor son para iOS 14.7.1, iPadOS 14.7.1 y macOS Big Sur 11.5.1. La actualización está disponible para productos, iPhone 6s y posteriores, todos los modelos de iPad Pro, iPad Air 2 y posteriores, iPad 5ta generación y posteriores, iPad mini 4 andy posteriores, y iPod touch.

Por mayor información al respecto se puede acceder a:
https://www.welivesecurity.com/la-es/2021/07/27/apple-parchea-zero-day-ios-ipados-macos/

Windows	Alerta sobre error que permite elevación de privilegios en Windows	PREVENCIÓN

Descripción

Especialistas en ciberseguridad advierten sobre una vulnerabilidad presente en Windows en Windows 10/11 que permite Escalamiento de Privilegios Locales (LPE).

"La vulnerabilidad, denominada HiveNightmware, también conocida como SeriousSAM, es el resultado de un conjunto de ACL "incorrecto" en los archivos del subárbol del registro en la carpeta C:\Windows\System32\Config. Esto permite que los usuarios habituales tengan acceso de lectura a SAM, SYSTEM, SECURITY y otros archivos críticos."

Afectados

Sistema operativo: Windows 10/11.

Vector de Ataque

Este archivo no puede estar disponible para los usuarios comunes, deberían tener acceso solamente aquellos usuarios con permiso de administrador y SYSTEM.

"Aunque las contraseñas estén cifradas, se puede crackear. Y si no es así, se pueden utilizar los hashes en crudo para acceder a sitios en red, por ejemplo, además de otras técnicas ya conocidas en las que se pueden utilizar como contraseña. Incluso se podría cambiar la contraseña de administrador conociendo solo el hash."

Los atacantes pueden utilizar a su favor el permiso de escritura erróneo, accediendo al SAM bloqueado, aunque no tengan acceso de administrador. Es importante destacar que teniendo acceso a SYSTEM y SECURITY también se puede tener control sobre el sistema objetivo.

Otra manera de lograr este ataque es acceder a la copia automática que hace el sistema de Shadow Copies de Windows, no solo con la SAM

"El bug fue encontrado mientras se probaba la próxima versión de Windows 11. Investigadores descubrieron que mientras Windows estaba restringiendo el acceso de los usuarios con pocos privilegios a esos archivos de configuración confidenciales, las copias de estos archivos también se guardaban en archivos de respaldo creados por Shadow Volume Copy, una función de Windows que crea instantáneas de archivos de computadora durante las operaciones del sistema de archivos."

Ya se han publicado varios códigos que facilitan la explotación y videos explicativos.

Remediación / Referencias

Microsoft ha publicado una mitigación en forma de comando que elimina ese permiso que debe ser ejecutado como administrador.

```
# Elimina el permiso
icacls %windir%\system32\config\*.* /inheritance:e
```

```
# Elimina la copia legible en Shadow Copies
vssadmin delete shadows /for=c: /Quiet
sc config vss start= disabled
```

Luego de cambiar los permisos y eliminar las Shadow Copies, ya no es posible realizar el volcado de la SAM y se puede volver a activar la Shadow Copies si se desea

Por mayor información al respecto se puede acceder a:
https://blog.segu-info.com.ar/2021/07/nueva-vulnerabilidad-de-elevacion-de.html

Conclusiones

Suele suceder con cada filtración de un nuevo sistema operativo, que se detecte la presencia de vulnerabilidades recientes, como sucedió con Windows 11, la nueva versión en desarrollo por parte de Microsoft para reemplazar Windows 10 y que tiene algunos componentes compartidos y otros nuevos.

De esta manera y a través de comparaciones de código, los crackers pueden inferir las porciones de código que tienen puntos de interrupción diferentes o más sencillos de "debuguear", es decir; de analizar los controles de seguridad en el sistema operativo en desarrollo, que no tiene todas las protecciones. Lo que permite reconocer el funcionamiento de los controles de ese sistema, pero también de su antecesor Windows 10, es por eso que esto suele invocar, y ha sucedido históricamente, lo que permite reconocer más brechas de seguridad por el conocimiento extra que genera por la liberación de un código del producto.

Es muy importante para las empresas que desarrollan software o mantienen secretos de propiedad intelectual, mantener garantías y resguardos con altos niveles de protección de datos. Muchas veces los equipos de trabajo no pueden acceder a la misma información del proyecto para no reconocerlo o filtrarlo por completo, por ello la separación de roles y ambientes es sumamente importante en ciberseguridad, en el manejo la información.

Las fallas de diseño suelen representar los mayores dolores de cabeza, ya que desde las primeras etapas del desarrollo de software se puede caer en interpretaciones, sesgos o faltas de requerimientos que impidan un control efectivo de la información que se desea proteger. Para esto los modelos de amenazas, análisis de arquitecturas de red y un seguimiento adecuado y seguro del ciclo de vida de software, es imprescindible para cualquier organización. Que requieran cualquier tipo de autorizacion especial respecto al acceso de la información, y de alguna manera estamos hablando de todas las organizaciones del mundo sin importar su tamaño o negocio.

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