Boletín de Ciberseguridad

Fecha de Publicación
24/05/2022- N.º 34

Mes de mayo
09/05/2022 - 24/05/2022

Datasec

Índice

Error de alta gravedad informado en la biblioteca de cliente OAuth 3
Microsoft lanza una corrección para el nuevo Zero-Day 4
VMware lanza parches para nuevas vulnerabilidades 5
Variante Sysrv Botnet secuestrando Windows y Linux con Crypto Miners 5
CISA recomienda parchear la vulnerabilidad F5 BIG-IP 6
Microsoft advierte sobre malware de robo de información 7
Conclusión: 9

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 mayo se destacan 6 noticias de relevancia: 5 sobre vulnerabilidades tecnológicas y 1 de prevención.

Aquellas noticias a tener especial recaudo son las siguientes:

Error de alta gravedad informado en la biblioteca de cliente OAuth

Google abordó una falla de alta gravedad en su biblioteca de cliente OAuth para Java que podría ser abusada por un actor malintencionado con un token comprometido para implementar cargas útiles arbitrarias.

VMware lanza parches para nuevas vulnerabilidades

VMware ha emitido parches para contener dos fallas de seguridad que afectan a Workspace ONE Access, Identity Manager y vRealize Automation que podrían explotarse en redes empresariales de puerta trasera.

CISA recomienda parchear la vulnerabilidad F5 BIG-IP

CISA agregó la falla F5 BIG-IP recientemente revelada a su Catálogo de Vulnerabilidades Explotadas Conocidas luego de informes de abuso activo en la naturaleza.

Java	**Error de alta gravedad informado en la biblioteca de cliente OAuth**	CRÍTICO

Descripción

Google abordó una falla de alta gravedad en su biblioteca de cliente OAuth para Java que podría ser abusada por un actor malintencionado con un token comprometido para implementar cargas útiles arbitrarias.

Estado

Rastreada como CVE-2021-22573, la vulnerabilidad tiene una calificación de 8,7 sobre 10 en cuanto a gravedad, y se relaciona con una omisión de autenticación en la biblioteca que se deriva de una verificación incorrecta de la firma criptográfica.

La biblioteca Java de código abierto, construida sobre la biblioteca de cliente HTTP de Google para Java, permite obtener tokens de acceso a cualquier servicio en la web que admita el estándar de autorización OAuth.

Google, en su archivo README para el proyecto en GitHub, señala que la biblioteca es compatible con el modo de mantenimiento y que solo corrige los errores necesarios, lo que indica la gravedad de la vulnerabilidad.

Remediación / Referencias

Se recomienda a los usuarios de la biblioteca google-oauth-java-client que actualicen a la versión 1.33.3, para mitigar cualquier riesgo potencial.

Por mayor información acceder a:
https://www.cert.gov.py/noticias/nuevo-error-de-criticidad-alta-reportada-en-oauth-de-google-para-java

Microsoft	Microsoft lanza una corrección para el nuevo Zero-Day	CRÍTICO

Descripción

Microsoft lanzó correcciones para 74 vulnerabilidades de seguridad, incluida una para un error de día cero que se está explotando activamente.

Estado

De los 74 problemas, siete se califican como críticos, 66 como Importantes y uno como de gravedad baja.

Estos abarcan: 24 ejecución remota de código (RCE), 21 elevación de privilegios, 17 divulgación de información y 6 vulnerabilidades de denegación de servicio, entre otras. Las actualizaciones se suman a 36 fallas parcheadas en el navegador Microsoft Edge.

El principal de los errores resueltos es CVE-2022-26925, una vulnerabilidad de suplantación de identidad que afecta a la Autoridad de Seguridad Local de Windows (LSA), que Microsoft describe como un "subsistema protegido que autentica e inicia sesión en el sistema local".

Las otras dos vulnerabilidades conocidas públicamente son las siguientes:

- CVE-2022-29972 (puntuación CVSS: 8,2) - Insight Software: CVE-2022-29972 Magnitud Simba Amazon Redshift ODBC Driver (también conocido como SynLapse)

- CVE-2022-22713 (puntuación CVSS: 5,6): vulnerabilidad de denegación de servicio de Windows Hyper-V

Remediación / Referencias

Es imperativo que los usuarios afectados apliquen las actualizaciones lo antes posible.

Por mayor información acceder a:
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-26925

vmware	**VMware lanza parches para nuevas vulnerabilidades**	CRÍTICO

Descripción

VMware ha emitido parches para contener dos fallas de seguridad que afectan a Workspace ONE Access, Identity Manager y vRealize Automation que podrían explotarse en redes empresariales de puerta trasera.

Estado

La primera de las dos fallas, rastreada como CVE-2022-22972 (puntuación CVSS: 9.8), se refiere a una omisión de autenticación que podría permitir que un actor con acceso de red a la interfaz de usuario obtenga acceso administrativo sin autenticación previa.

CVE-2022-22973 (puntaje CVSS: 7.8), el otro error, es un caso de escalada de privilegios locales que podría permitir que un atacante con acceso local eleve los privilegios al usuario "raíz" en dispositivos virtuales vulnerables.

La divulgación sigue a una advertencia de la Agencia de Infraestructura y Seguridad Cibernética de EE. UU. (CISA) de que los grupos de amenazas persistentes avanzadas (APT) están explotando CVE-2022-22954 y CVE-2022-22960, otras dos fallas de VMware que se solucionaron a principios del mes pasado, por separado y en combinación.

Además de eso, los actores de amenazas han implementado herramientas posteriores a la explotación, como el shell web Dingo J-spy en al menos tres organizaciones diferentes.

Remediación / Referencias

Si bien no se ha visto ninguna evidencia de que las vulnerabilidades hayan sido explotadas en la naturaleza, se recomienda encarecidamente que aplique los parches para eliminar las amenazas potenciales.

Por mayor información acceder a:
https://www.vmware.com/security/advisories/VMSA-2022-0014.html

Microsoft	**Variante Sysrv Botnet secuestrando Windows y Linux con Crypto Miners**	CRÍTICO

Descripción

Microsoft advierte sobre una nueva variante de la botnet srv que explota múltiples fallas de seguridad en aplicaciones web y bases de datos para instalar mineros de monedas en sistemas Windows y Linux.

Estado

Se dice que Sysrv-K, arma una serie de exploits para obtener el control de los servidores web. Esto también incluye CVE-2022-22947 (puntaje CVSS: 10.0), una vulnerabilidad de inyección de código en Spring Cloud Gateway que podría explotarse para permitir la ejecución remota arbitraria en un host remoto a través de una solicitud creada con fines malintencionados.

Un diferenciador clave es que Sysrv-K busca archivos de configuración de WordPress y sus copias de seguridad para obtener las credenciales de la base de datos, que luego se utilizan para secuestrar servidores web. También se dice que actualizó sus funciones de comunicación de comando y control para hacer uso de un Telegram Bot.

Remediación / Referencias

Además de proteger los servidores expuestos a Internet, Microsoft también aconseja a las organizaciones que apliquen actualizaciones de seguridad de manera oportuna.

Por mayor información acceder a:
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22947

	CISA recomienda parchear la vulnerabilidad F5 BIG-IP	CRÍTICO

Descripción

CISA agregó la falla F5 BIG-IP recientemente revelada a su Catálogo de Vulnerabilidades Explotadas Conocidas luego de informes de abuso activo en la naturaleza.

Estado

La falla, a la que se le asignó el identificador CVE-2022-1388 (puntaje CVSS: 9.8), se refiere a un error crítico en el punto final BIG-IP iControl REST que proporciona a un adversario no autenticado un método para ejecutar comandos arbitrarios del sistema.

F5 anunció parches y mitigaciones para la falla el 4 de mayo, pero ha sido objeto de explotación en estado salvaje durante la última semana, con atacantes que intentan instalar un shell web que otorga acceso de puerta trasera a los sistemas objetivo.

Para empeorar las cosas, ha surgido evidencia de que la falla de ejecución remota de código se está utilizando para borrar por completo los servidores objetivo como parte de ataques destructivos para dejarlos inoperables mediante la emisión de un comando " rm -rf /* " que elimina recursivamente todos los archivos.

Remediación / Referencias

Se recomienda a todos los usuarios, parchear todos los sistemas contra el problema antes del 31 de mayo de 2022.

Por mayor información acceder a:
https://www.cisa.gov/uscert/ncas/alerts/aa22-138a

Microsoft	**Microsoft advierte sobre malware de robo de información**	PREVENCIÓN

Descripción

Microsoft advierte sobre una amenaza emergente dirigida a las billeteras de criptomonedas conectadas a Internet, lo que indica un cambio en el uso de monedas digitales en los ataques cibernéticos.

Estado

La nueva amenaza conocida como "cryware", provocó que los ataques resultaran en el robo irreversible de monedas virtuales mediante transferencias fraudulentas a una billetera controlada por un adversario.

El cryware abarca las siguientes amenazas:

- Cryptojackers que consumen subrepticiamente los recursos del dispositivo de un objetivo para extraer criptomonedas
- Campañas de ransomware que utilizan criptomonedas como pago de rescate para evitar la detección
- Ladrones de información (p. ej., Mars Stealer , RedLine Stealer , Arkei y Raccoon) que se actualizan cada vez más para desviar datos de billetera activa junto con otra información valiosa almacenada en el sistema, y
- ClipBankers (también conocidos como clippers) que roban criptomonedas durante las transacciones al monitorear el portapapeles y reemplazar la dirección de la billetera original con la dirección del atacante.

Dichos ataques de robo de información tienen como objetivo extraer datos de billetera activa, como claves privadas, frases iniciales y direcciones de billetera, lo que permite que el actor de amenazas inicie transacciones deshonestas y mueva fondos a otra billetera

Remediación / Referencias

Se recomienda a los usuarios y organizaciones que bloqueen las billeteras activas cuando no estén comerciando, desconecten los sitios conectados a una billetera, eviten almacenar claves privadas en texto sin formato y verifiquen el valor de la dirección de la billetera al copiar y pegar la información.

Para saber más invitamos a visitar el siguiente sitio:
https://www.microsoft.com/security/blog/2022/05/17/in-hot-pursuit-of-cryware-defending-hot-wallets-from-attacks/

Conclusión:

Una nueva quincena cargada con novedades en diferentes soluciones populares o mainstream. Hoy en esta conclusión vamos a abordar porqué existen tantas recomendaciones enfocadas al seguimiento y actualización de parches mayores o menores de software; esta actividad que cada vez es más usual y conocida por toda persona que se acerca a cualquier tecnología, ya que la misma evoluciona con la misma renovación de los productos que se comercian. La vorágine de nuevas actualizaciones ha hecho que cada vez más corporaciones busquen soluciones robustas y profilácticas; que incorporen las mismas soluciones de software con actualizaciones confiables, o bien en las integraciones de software.
De otra forma las actualizaciones no suelen ser seguidas o aplicadas y se exponen a una cantidad de riesgos importantes.

Estas actualizaciones, son cada vez más relevantes de incorporarlas a medida que los adversarios aumentan en cantidad y capacidad, y las defensas sobre algunos aspectos siempre se pueden reforzar para trabajar con seguridad y tranquilidad.

Finalmente destacamos estar en constante conocimiento respecto a intentos de fraudes activos, actualización de vulnerabilidades recién descubiertas, así como las características y especificaciones de los ransomware que prevalecen en la actualidad.