Boletín de Ciberseguridad N°68

Fecha de publicación: 09/10/2023

Mes de Octubre

29/09/2023 – 09/10/2023

Datasec

BOLETÍN DE CIBERSEGURIDAD

Indice

Introducción....3

Se lanza parche de seguridad para dos nuevas fallas en la biblioteca Curl....5

CISA advierte sobre vulnerabilidades de JetBrains y Windows....5

Cisco lanza un parche urgente....8

Qualcomm lanza parche....9

Apple lanza parches de seguridad....10

Conclusiones....11

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 octubre se destacan 5 noticias de relevancia: 2 sobre vulnerabilidades tecnológicas, y 3 de prevención.

Aquellas noticias a tener especial recaudo son las siguientes:

CISA advierte sobre vulnerabilidades de JetBrains y Windows

CISA agregó el miércoles dos fallas de seguridad a su catálogo de Vulnerabilidades Explotadas Conocidas (KEV) debido a una explotación activa, mientras que eliminó cinco errores de la lista debido a la falta de evidencia adecuada.

Cisco lanza un parche urgente

Cisco ha lanzado actualizaciones para abordar una falla de seguridad crítica que afecta a Emergency Responder y que permite a atacantes remotos no autenticados iniciar sesión en sistemas susceptibles utilizando credenciales codificadas.

Apple lanza parches de seguridad

Apple lanzó el miércoles parches de seguridad para abordar una nueva falla de día cero en iOS y iPadOS que, según dijo, ha sido explotada activamente en la naturaleza.

Vulnerabilidad Crítica

curl command line tool and library for transferring data with URLs	Se lanza parche de seguridad para dos nuevas fallas en la biblioteca Curl	CRÍTICO

Descripción

Los mantenedores de la biblioteca Curl han publicado una advertencia sobre dos vulnerabilidades de seguridad que se espera que se solucionen como parte de una próxima actualización que se lanzará el 11 de octubre de 2023.

Estado

Se han retenido detalles adicionales sobre los problemas y los rangos exactos de versiones afectadas debido a la posibilidad de que la información pueda usarse para "ayudar a identificar el problema (área) con una precisión muy alta".

Curl, desarrollado por libcurl, es una popular herramienta de línea de comandos para transferir datos especificados con sintaxis de URL. Admite una amplia gama de protocolos como FTP(S), HTTP(S), IMAP(S), LDAP(S), MQTT, POP3, RTMP(S), SCP, SFTP, SMB(S), SMTP(S), TELNET, WS y WSS.

Remediación / Referencias

Se recomienda inventariar y escanear urgentemente todos los sistemas que utilizan curl y libcurl, anticipando la identificación de versiones potencialmente vulnerables una vez que se revelen los detalles con el lanzamiento de Curl 8.4.0 el 11 de octubre.

Por mayor información acceder a: https://curl.se/changes.html

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY CISA	CISA advierte sobre vulnerabilidades de JetBrains y Windows	CRÍTICO

Descripción

CISA agregó el miércoles dos fallas de seguridad a su catálogo de Vulnerabilidades Explotadas Conocidas (KEV) debido a una explotación activa, mientras que eliminó cinco errores de la lista debido a la falta de evidencia adecuada.

Estado

Las vulnerabilidades recién agregadas se encuentran a continuación:

- CVE-2023-42793 (puntuación CVSS: 9,8) - Vulnerabilidad de omisión de autenticación de JetBrains TeamCity
- CVE-2023-28229 (puntuación CVSS: 7.0): vulnerabilidad de escalada de privilegios del servicio de aislamiento de claves CNG de Microsoft Windows

CVE-2023-42793 se relaciona con una vulnerabilidad crítica de omisión de autenticación que permite la ejecución remota de código en TeamCity Server. Los datos recopilados por GreyNoise han revelado intentos de explotación dirigidos a la falla desde 74 direcciones IP únicas hasta la fecha.

Por otro lado, CVE-2023-28229 es una falla de alta gravedad en el Servicio de aislamiento de claves criptográficas de próxima generación (CNG) de Microsoft Windows que permite a un atacante obtener privilegios de SISTEMA limitados específicos.

Remediación / Referencias

Las agencias del Poder Ejecutivo Civil Federal (FCEB) deben aplicar los parches proporcionados por los proveedores antes del 25 de octubre de 2023 para proteger sus redes contra posibles amenazas.

Por más información, acceder a:

https://www.cisa.gov/news-events/alerts/2023/10/04/cisa-adds-two-known-exploited-vulnerabilities-catalog-removes-five-kevs

Prevención

cisco	Cisco lanza un parche urgente	PREVENCIÓN

Descripción

Cisco ha lanzado actualizaciones para abordar una falla de seguridad crítica que afecta a Emergency Responder y que permite a atacantes remotos no autenticados iniciar sesión en sistemas susceptibles utilizando credenciales codificadas.

Estado

La vulnerabilidad, rastreada como CVE-2023-20101 (puntuación CVSS: 9,8), se debe a la presencia de credenciales de usuario estáticas para la cuenta raíz que, según la compañía, generalmente se reserva para su uso durante el desarrollo.

El problema afecta a Cisco Emergency Responder versión 12.5(1)SU4 y se solucionó en la versión 12.5(1)SU5. Otras versiones del producto no se ven afectadas.

La divulgación se produce menos de una semana después de que Cisco advirtiera sobre un intento de explotación de una falla de seguridad en su software IOS y su software IOS XE (CVE-2023-20109 , puntuación CVSS: 6,6) que podría permitir a un atacante remoto autenticado lograr la ejecución remota de código en sistemas afectados.

Remediación / Referencias

Se recomienda a los clientes que actualicen a la última versión para mitigar posibles amenazas.

Por mayor información acceder a:

https://devel.group/blog/cisco-emite-solucion-urgente-para-el-error-de-omision-de-autenticacion-que-afecta-a-la-plataforma-broadworks/

Qualcomm	Qualcomm lanza parche	PREVENCIÓN

Descripción

El fabricante de chips Qualcomm ha publicado actualizaciones de seguridad para abordar 17 vulnerabilidades en varios componentes, al tiempo que advierte que otros tres días cero han sido explotados activamente.

Estado

De los 17 defectos, tres están clasificados como críticos, 13 como altos y uno como de gravedad media.

Las actualizaciones de Qualcomm de octubre de 2023 también abordan tres problemas críticos, aunque no hay evidencia de que se haya abusado de ellos en la naturaleza:

- CVE-2023-24855 (puntuación CVSS: 9,8): corrupción de la memoria en el módem al procesar la configuración relacionada con la seguridad antes de AS Security Exchange.
- CVE-2023-28540 (puntuación CVSS: 9,1): problema criptográfico en el módem de datos debido a una autenticación incorrecta durante el protocolo de enlace TLS.
- CVE-2023-33028 (puntuación CVSS: 9,8): corrupción de la memoria en el firmware de WLAN al realizar una copia de la memoria del caché pmk.

Remediación / Referencias

Se recomienda a los usuarios que apliquen las actualizaciones de los fabricantes de equipos originales (OEM) tan pronto como estén disponibles.

Por mayor información acceder a:

https://nvd.nist.gov/vuln/detail/CVE-2023-24855

	Apple lanza parches de seguridad	PREVENCIÓN

Descripción

Apple lanzó el miércoles parches de seguridad para abordar una nueva falla de día cero en iOS y iPadOS que, según dijo, ha sido explotada activamente en la naturaleza.

Estado

Registrada como CVE-2023-42824, un atacante local podría abusar de la vulnerabilidad del kernel para elevar sus privilegios. El fabricante del iPhone dijo que abordó el problema con controles mejorados.

Si bien actualmente se desconocen detalles adicionales sobre la naturaleza de los ataques y la identidad de los actores de amenazas que los perpetran, la explotación exitosa probablemente depende de que un atacante ya haya obtenido un punto de apoyo inicial por algún otro medio.

La última actualización de Apple también resuelve CVE-2023-5217 que afecta al componente WebRTC, que Google describió la semana pasada como un desbordamiento de búfer basado en montón en el formato de compresión VP8 en libvpx.

Remediación / Referencias

Se recomienda a los usuarios que corren el riesgo de ser atacados que habiliten el modo de bloqueo para reducir la exposición a exploits de software espía mercenario.

Por más información acceder a:

https://nvd.nist.gov/vuln/detail/CVE-2023-42824

Conclusiones

Las recomendaciones generales siguen estando enfocadas en los posibles riesgos que se puedan generar a nivel de las conexiones remotas de los teletrabajadores.

Se recomienda actualizar los conectores VPN que dispongan, como contar con configuraciones seguras que eviten y/o puedan evaluar el estado general de los endpoints o sistemas que se conectan a la VPN.

Es decir, es muy valioso poder contar en estas situaciones con validadores de higiene general de equipamientos remotos, tanto a nivel de que los sistemas operativos estén actualizados y con los parches de seguridad al día, así como también que los controles de seguridad tales como los antivirus estén también habilitados y funcionando. Esto previene en gran medida los posibles abusos o compromisos que se puedan generar a nivel de los usuarios remotos a los cuales le damos acceso a la red informática de la organización.

Existen varias soluciones técnicas a este nivel tanto como Fortinet con su Forticlient Health Check como soluciones tales como Duo Security Device Health, entre otros.

Esto mejorará la postura de ciberseguridad, como también habilitar la autenticación con dobles factores lo que aumenta en gran medida la pérdida de accesos de estos usuarios remotos y refuerza mucho la protección.

Desde el equipo de Datasec seguimos protegiendo la seguridad de nuestros clientes, socios y colaboradores.

¡Sigan protegiéndose!