Boletín de Ciberseguridad N°65

Fecha de publicación: 28/08/2023

Mes de agosto

14/08/2023 – 28/08/2023

Datasec

BOLETÍN DE CIBERSEGURIDAD

Indice

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

Aquellas noticias a tener especial recaudo son las siguientes:

Se agregó una falla crítica de Adobe ColdFusion

CISA ha agregado una falla de seguridad crítica en Adobe ColdFusion a su catálogo de vulnerabilidades explotadas conocidas (KEV), basándose en evidencia de explotación activa.

Se detecta nueva vulnerabilidad de WinRAR

Se ha revelado una falla de seguridad de alta gravedad en la utilidad WinRAR que podría ser potencialmente explotada por un actor de amenazas para lograr la ejecución remota de código en sistemas Windows.

CISA agrega un defecto de Citrix ShareFile al catálogo KEV

CISA ha agregado una falla de seguridad crítica en el controlador de zonas de almacenamiento Citrix ShareFile a su catálogo de vulnerabilidades explotadas conocidas (KEV), basándose en evidencia de explotación activa en estado salvaje.

Vulnerabilidad Crítica

Se agregó una falla crítica de Adobe ColdFusion

CRÍTICO

Descripción

CISA ha agregado una falla de seguridad crítica en Adobe ColdFusion a su catálogo de vulnerabilidades explotadas conocidas (KEV), basándose en evidencia de explotación activa.

Estado

La vulnerabilidad, catalogada como CVE-2023-26359 (puntuación CVSS: 9,8), se relaciona con una falla de deserialización presente en Adobe ColdFusion 2018 (Actualización 15 y anteriores) y ColdFusion 2021 (Actualización 5 y anteriores) que podría resultar en la ejecución de código arbitrario en el contexto del usuario actual sin requerir ninguna interacción.

Adobe lo parchó como parte de las actualizaciones publicadas en marzo de 2023. Al momento de escribir este artículo, no está claro de inmediato cómo se está abusando de la falla en la naturaleza.

Dicho esto, el desarrollo se produce más de cinco meses después de que CISA incluyera otra falla que afectaba al mismo producto (CVE-2023-26360) en el catálogo de KEV. Adobe dijo que es consciente de la debilidad que se está explotando en "ataques muy limitados" dirigidos a ColdFusion.

Remediación / Referencias

Se deben aplicar los parches necesarios antes del 11 de septiembre de 2023 para proteger las redes contra posibles amenazas.

Por mayor información acceder a:

https://windows.atsit.in/es/16864/

Se detecta nueva vulnerabilidad de WinRAR

CRÍTICO

Descripción

Se ha revelado una falla de seguridad de alta gravedad en la utilidad WinRAR que podría ser potencialmente explotada por un actor de amenazas para lograr la ejecución remota de código en sistemas Windows.

Estado

Registrada como CVE-2023-40477 (puntuación CVSS: 7,8), la vulnerabilidad se ha descrito como un caso de validación inadecuada al procesar volúmenes de recuperación.

La explotación exitosa de la falla requiere la interacción del usuario, ya que se debe atraer al objetivo para que visite una página maliciosa o simplemente abra un archivo comprimido con trampa explosiva.

La última versión también soluciona un segundo problema en el que "WinRAR podría iniciar un archivo incorrecto después de que un usuario hiciera doble clic en un elemento en un archivo especialmente diseñado". Al investigador del Grupo IB, Andrey Polovinkin, se le atribuye el mérito de informar del problema.

Remediación / Referencias

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

Por mayor información acceder a:

https://www.incibe.es/ciudadania/avisos/actualiza-winrar-la-version-623-para-solucionar-la-vulnerabilidad

	CISA agrega un defecto de Citrix ShareFile al catálogo KEV	CRÍTICO

Descripción

CISA ha agregado una falla de seguridad crítica en el controlador de zonas de almacenamiento Citrix ShareFile a su catálogo de vulnerabilidades explotadas conocidas (KEV), basándose en evidencia de explotación activa en estado salvaje.

Estado

Registrada como CVE-2023-24489 (puntuación CVSS: 9,8), la deficiencia se ha descrito como un error de control de acceso inadecuado que, si se explota con éxito, podría permitir que un atacante no autenticado comprometa instancias vulnerables de forma remota.

El problema tiene su origen en el manejo de las operaciones criptográficas por parte de ShareFile, lo que permite a los adversarios cargar archivos arbitrarios, lo que resulta en la ejecución remota de código.

Se desconoce la identidad de los actores de amenazas detrás de los ataques, aunque la banda de ransomware Cl0p se ha interesado especialmente en aprovechar los días cero en soluciones de transferencia de archivos administradas como Accellion FTA, SolarWinds Serv-U, GoAnywhere MFT y Progress MOVEit. Transferencia en los últimos años.

Remediación / Referencias

Se publicó una solución para CVE-2023-24489 el 11 de mayo de 2023, con la versión 5.11.24, un mes antes de que se publicará el aviso de seguridad el 13 de junio de 2023.

Por mayor información acceder a:

https://www.cisa.gov/news-events/alerts/2023/08/16/cisa-adds-one-known-exploited-vulnerability-catalog

Prevención

JUNOS	**Nuevas fallas de Juniper Junos OS**	**PREVENCIÓN**

Descripción

Se ha lanzado una actualización de seguridad "fuera de ciclo" para abordar múltiples fallas en el componente J-Web de Junos OS que podrían combinarse para lograr la ejecución remota de código en instalaciones susceptibles.

Estado

Las cuatro vulnerabilidades tienen una calificación CVSS acumulativa de 9,8, lo que las convierte en críticas en cuanto a gravedad. Afectan a todas las versiones de Junos OS en las series SRX y EX.

La interfaz J-Web permite a los usuarios configurar, administrar y monitorear dispositivos Junos OS. Una breve descripción de las fallas es la siguiente:

- CVE-2023-36844 y CVE-2023-36845 (puntuaciones CVSS: 5.3): dos vulnerabilidades de modificación de variables externas de PHP en J-Web de Juniper Networks Junos OS en las series EX y SRX permiten que un atacante basado en red no autenticado controle ciertos, variables ambientales importantes.
- CVE-2023-36846 y CVE-2023-36847 (puntuaciones CVSS: 5,3): dos autenticaciones faltantes para vulnerabilidades de funciones críticas en Juniper Networks Junos OS en las series EX y SRX permiten que un atacante basado en red no autenticado cause un impacto limitado en la integridad del sistema de archivos.
-

Las vulnerabilidades se han solucionado en las siguientes versiones:

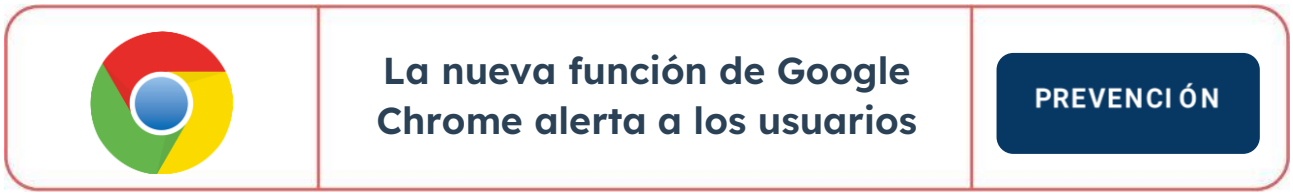
- Serie EX: versiones de Junos OS 20.4R3-S8, 21.2R3-S6, 21.3R3-S5, 21.4R3-S4, 22.1R3-S3, 22.2R3-S1, 22.3R2-S2, 22.3R3, 22.4R2-S1, 22.4 R3 y 23.2R1
- Serie SRX: versiones de Junos OS 20.4R3-S8, 21.2R3-S6, 21.3R3-S5, 21.4R3-S5, 22.1R3-S3, 22.2R3-S2, 22.3R2-S2, 22.3R3, 22.4R2-S1, 22.4 R3 y 23.2R1

Remediación / Referencias

Se recomienda a los usuarios que apliquen las correcciones necesarias para mitigar posibles amenazas de ejecución remota de código. Como solución alternativa, Juniper Networks sugiere que los usuarios deshabiliten J-Web o limiten el acceso sólo a hosts confiables.

Por mayor información acceder a:

https://socradar.io/exploiting-multiple-j-web-vulnerabilities-to-enable-unauthenticated-remote-code-execution-in-juniper-os-cve-2023-36844-through-cve-2023-36847/



Descripción

Google ha anunciado planes para agregar una nueva función en la próxima versión de su navegador web Chrome para alertar proactivamente a los usuarios cuando una extensión que hayan instalado haya sido eliminada de Chrome Web Store.

Estado

La función, que se lanzará junto con Chrome 117, permite a los usuarios recibir notificaciones cuando un desarrollador cancela la publicación de un complemento, lo elimina por violar la política de Chrome Web Store o lo marca como malware.

El desarrollo se produce cuando la compañía dijo que actualizará automáticamente todas las navegaciones URL https:// a https:// incluso cuando los usuarios hagan clic en un enlace que declara explícitamente https://. La función se está probando actualmente en Chrome 115 y se espera que se implemente pronto.

Google también dijo que mostrará una advertencia a partir de mediados de septiembre de 2023 cuando los usuarios intenten descargar archivos de alto riesgo mientras tienen una conexión insegura.

Remediación / Referencias

Los usuarios pueden habilitar el modo HTTPS-First habilitando "Usar siempre conexiones seguras" en la configuración de seguridad de Chrome (chrome://settings/security).

Por mayor información acceder a:

https://www.google.com/intl/es_es/chrome/?brand=YTUH&gclid=Cj0KCQjwi7GnBhDXARIsAFLvH4mtQC86i3lYzdyvbi2jsGYHAEuJOmqbc-Mnh4llcWwGHjj1A5xmS2UaAqNoEALw_wcB&gclsrc=aw.ds

Conclusiones

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

También habilitar la autenticación con dobles factores 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!