Informe de Inteligencia de amenazas

CVE- 2023-41773 – 11 de octubre de 2023

Resumen

CVE- 2023-41773, publicado el 5 de octubre de 2023 , hace referencia a un informe de vulnerabilidad relacionado con la ejecución remota de código (RCE) y la ruta Fallo transversal en la versión 2.4.49 de Apache.

Se trata de una vulnerabilidad grave cuyas vulnerabilidades se observaron mucho antes del 5 de octubre. Análisis forense digital y respuesta a incidentes (DFIR) de los sistemas afectados debe comenzar lo antes posible.

Recomendaciones

Actividades de respuesta a incidentes

• Iniciar actividades forenses inmediatamente para determinar completamente el alcance del impacto.
• Determinar si las notificaciones son necesarias

Respuesta de seguridad operativa

• Garantizar que la aplicación de parches en los sistemas vulnerables se realice lo antes posible
• Considere limitar la exposición de la red a sistemas no críticos.

Respuesta de detección de amenazas

• Aumentar las alertas de entradas anómalas del registro del sistema
• Incrementar el monitoreo de fuentes OSINT emergentes (por ejemplo, Twitter)

Resultados clave

• Los atacantes han obtenido acceso al archivo /etc/passwd en al menos un sistema. Esto expone nombres de usuario, algún grupode información y cierta información de la ruta del sistema de archivos. No expone contraseñas.
• Apache v2.4.50 es una solución incompleta (consulte CVE- 2023-42013 1). Recomendar actualizar a v2.4.51.
• Si no es posible realizar la actualización, establecer "Requerir todo denegado" en los permisos de directorio de la configuración de Apache y mitigar la amenaza.
• Los intentos de explotación de esta vulnerabilidad son anteriores al CVE al menos tres semanas (los registros muestran un análisis a mediados de septiembre).
• El código de explotación está disponible públicamente en Twitter y GitHub desde el 5 de octubre.

Detalles de CVE y parches

El 5 de octubre de 2023 , se lanzó CVE- 2023-41773 2 . La divulgación detalla una vulnerabilidad trivialmente explotable en Apache v2.4.49, un paquete de software de servidor web común.
La Fundación Apache lanzó un parche para las versiones 2.4.49 y 2.4.50 el 5 de octubre. Se evaluó este parche de Apache v2.4.49 a v2.4.50 como una solución 4 incompleta ya que no abordaba una vulnerabilidad que aún podría

explotarse. Cualquier sistema que se haya actualizado a v2.4.50 es necesario actualizar más a v2.4.51. Además, estos sistemas deben revisarse para detectar signos de explotación debido a la vulnerabilidad en v2.4.50.

Detalles de explotación

El exploit en sí es trivial de realizar y una situación de alto riesgo para cualquier sistema Apache v2.4.49 y v2.4.50. Detalles sobre el exploit están disponibles a través de Twitter y GitHub que muestran la explotación. Para explotar esta vulnerabilidad, un atacante sólo necesita pasar un GET solicitud a un servidor web vulnerable. Por ejemplo, la siguiente línea tomará el archivo /etc/passwd:

GET /cgi-bin/.%2e/%2e%2e/%2e%2e/%2e%2e/etc/passwd

Es posible explotar esta vulnerabilidad mediante solicitudes GET, solicitudes POST y probablemente utilizando otros verbos, como solicitudes HEAD, puede resultar en la divulgación de información.
Esta vulnerabilidad también puede provocar la ejecución remota de código (RCE) para determinadas cadenas y en algunos casos. Por ejemplo, el siguiente solicitud dará como resultado RCE para sistemas vulnerables mediante la ejecución del comando 'id':

GET /cgi-bin/.%2e/%2e%2e/%2e%2e/%2e%2e/bin/sh id

La configuración predeterminada para Apache v2.4.49 no es vulnerable. Se necesitan los siguientes ajustes de configuración predeterminados para el sistema para no ser vulnerable:

<Directorio />
Requerir todo **denegado**
</Directorio>

Fuentes de inteligencia de código abierto

Esta vulnerabilidad fue ampliamente cubierta en las redes sociales y los detalles de la vulnerabilidad y el código de ejemplo son prolíficos. El siguiente ejemplo reflejan algunos de esos hallazgos.

Twitter

Figura 1: Tweet que muestra el método para escanear hosts y determinar la vulnerabilidad a CVE 2023 41773

Este tweet muestra un script de una línea efectivo para escanear una lista de objetivos e intentar recuperar el archivo /etc/passwd del host. En si tiene éxito, imprime "Vulnerable" y, en caso de error, "No vulnerable". Esto demuestra que la exfiltración de datos es posible en sistemas vulnerables utilizando el error de recorrido de ruta. Este script no debe ejecutarse en sistemas de destino que no sean propiedad ni estén controlados por la parte que ejecuta el script.

Dado que utiliza la vulnerabilidad para extraer datos, su legalidad puede ser cuestionable en algunas jurisdicciones.
El tweet anterior se publicó a las 11:34 a. m. (UTC -4) del 5 de octubre de 2023 . El primer aviso público de esta vulnerabilidad puede haber sido una publicación de la lista de correo [6] de las 09:03:14 UTC del 5 de octubre de 2023.

Twitter cont.

Figura 2: Tweet que vincula CVE 2023 41773 y CVE 2023 42013

El enlace de la Figura 2 nos lleva a una breve publicación de blog que resume rápidamente el estado del escaneo continuo de la vulnerabilidad. El comentario se reproduce íntegramente a continuación:
"El 7 de octubre de 2023 , la Apache Software Foundation lanzó la versión 2.4.51 del servidor Apache HTTP para abordar Path Vulnerabilidades de ejecución remota y transversal de código (CVE- 2023-41773 , CVE-2023-42013) en el servidor HTTP Apache 2.4.4 y 2.4.50. Estas vulnerabilidades han sido explotadas en la naturaleza.
CISA también está observando un escaneo continuo de sistemas vulnerables, que se espera que se acelere, lo que probablemente conduzca a la explotación.
CISA insta a las organizaciones a aplicar parches de inmediato si aún no lo han hecho; esto no puede esperar hasta después del fin de semana festivo".

Fuente: https://us-cert.cisa.gov/ncas/current-activity/ 2023 /10/07/apache-releases-http-server-version-2451-address-vulnerabilities
Figura 3: Tweet que muestra la búsqueda de Shodan para Apache 2.4.49

La Figura 3 muestra una captura de pantalla del número total de servicios vulnerables a nivel mundial, detectados por Shodan el 5 de octubre de 2023 .
La importancia de los datos muestra que posiblemente haya 112.758 servicios de escucha vulnerables.
Comentario: Este exploit tuvo mucha cobertura en Twitter. Los tweets presentados sólo representan una fracción muy pequeña del total cobertura. Los tweets llegaron muy cerca del momento de la publicación de los avisos públicos sobre la vulnerabilidad. El tiempo hasta la prueba del concepto que se hace público aquí es muy rápido. Esto es típico de este tipo de exploit y demuestra la relevancia de utilizar Twitter.

GitHub

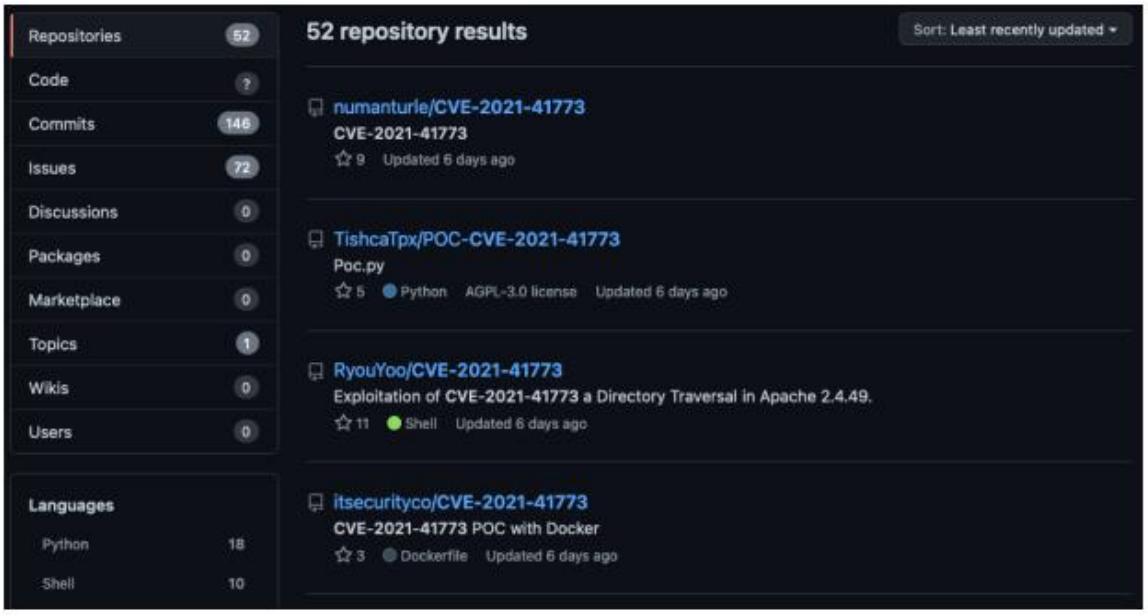

Figura 4: Muestra 52 repositorios de GitHub disponibles para CVE- 2023-41773 el 11 de octubre

GitHub muestra muchos exploits y scripts diferentes en repositorios públicos. Nuestra captura de pantalla anterior muestra que había 52 diferentes repositorios que coincidieron con “CVE- 2023-41773 ” como término de búsqueda. Varios proyectos estuvieron disponibles el 5 de octubre.

Comentario: Los datos de GitHub no contribuyen significativamente a nuestra comprensión obtenida de Twitter. Sirve para confirmar la información de Twitter y muestra tiempos cortos similares desde que la vulnerabilidad se hace pública hasta que el código POC está disponible. Algunos de los proyectos dentro de GitHub pueden ser útiles para escanear nuestra infraestructura y determinar nuestra exposición. Deberíamos validar el código benigno antes de confiar en cualquiera de estas herramientas para escanear nuestra infraestructura.

Shodan

Figura 5: Búsqueda de Shodan de “Apache/2.4.49” del 11 de octubre

Las búsquedas de Shodan realizadas el 11 de octubre muestran 67.891 servicios expuestos que se identifican como Apache v2.4.49.

Figura 6: Búsqueda de Shodan de "Apache/2.4.50" del 11 de octubre

Una búsqueda de “Apache/2.4.50” realizada el 11 de octubre muestra 13.568 servicios de escucha.

Comentario: Los resultados de Shodan cuentan cada par de IP y PUERTO como un informe distinto para el campo "Resultados totales". Es común que un solo sistema para ejecutar Apache en el puerto 80 y el puerto 443. En algunos casos, un solo sistema puede ejecutar Apache en muchos más puertos. Esto causa los “Resultados totales” deben ser mayores que el recuento único de hosts.

La detección de versión se puede suprimir mediante la configuración de Apache. Esto puede causar que los “Resultados totales” cuenten por debajo del total servicios que escuchan y ejecutan nuestras versiones de destino.
Dadas estas limitaciones, es razonable estimar que el recuento de hosts únicos puede ser aproximadamente el 50 % de los “Resultados totales” para este buscar. Por lo tanto, a partir del 11 de octubre, podemos estimar que habrá aproximadamente 33.500 hosts únicos ejecutando Apache v2.4.49 y aproximadamente 6.750 ejecutando Apache v2.4.50.
Todos estos sistemas representan sistemas expuestos públicamente en un estado que es trivial de explotar. Estos bien pueden usarse para más uso malicioso, que es un resultado común para este tipo de exploit y vulnerabilidad.

Resumen y recomendaciones

CVE- 2023-41773 ha impactado a nuestra organización y puede continuar impactándonos hasta que tomemos medidas de mitigación. Los registros muestran nuestra sistemas explotados con éxito.
Para estos activos, esperamos que la exfiltración o explotación de datos ya haya ocurrido. Esfuerzos inmediatos para identificar, aislar y se recomienda mitigar esta vulnerabilidad para todos los servidores Apache v2.4.49. Estos servidores deben parchearse a v2.4.51 o posterior después se toman imágenes de los sistemas para el equipo DFIR. La organización no parece tener servidores Apache v2.4.50, pero si se encuentra alguno, estos deben actualizarse a la versión 2.4.51 o posterior. Si es necesario retrasar la aplicación de parches en estos servidores, podemos mitigar el impacto de esto vulnerabilidad estableciendo la **directiva "Requerir todo denegado".**
Además, recomendamos DFIR completo para hosts vulnerables a este problema. Dado que la RCE es posible, podría haber un mayor impacto más allá de eso ya anotado.