CONCIBER
Comité Nacional de Seguridad Cibernética

ALERTA

Vulnerabilidad en el Servidor Apache HTTP

Fecha: **11/10/2022**

Problemática: **Path Traversal Zero-Day en Apache HTTP Server**

Correlativo: **AA-0039**

Institución / Sector: **Instituciones Públicas y Privadas**

CONTEXTO

Apache Software Foundation emitió un comunicado por medio de sus canales oficiales, sobre la vulnerabilidad identificada como CVE-2021-41773, encontrada en el servidor Apache HTTP Server para plataformas Unix, Microsoft Windows, Macintosh y otras. comprometidos por un tercero.
La explotación de esta vulnerabilidad conlleva a que los servicios se vean comprometidos por un tercero.

Nivel de priorización

Prioridad Urgente / No Urgente	Actualización Seguimiento/Preventiva/Resiliente
Urgente	Preventiva

Matriz de Evaluación

Riesgo Alto/ Medio/ Bajo	Nivel de Afectación		
	Integridad	Disponibilidad	Confidencialidad
Alto	Medio	Alta	Medio

SITUACIÓN

De acuerdo a la información obtenida a raíz de la investigación realizada por el Centro Estratégico de Monitoreo – CEM, un ciberdelincuente al explotar la vulnerabilidad podría usar la técnica de ataque transversal de ruta para asignar URL a archivos fuera de los directorios configurados por directivas similares al Alias. Si los archivos fuera de estos directorios no están protegidos por la configuración predeterminada habitual "requerir todos los denegados", estas solicitudes pueden tener éxito. Si los scripts CGI también están habilitados para estas rutas con alias, esto podría permitir la ejecución remota de código.

Versión afectada:

- **Esta vulnerabilidad solo afecta a la versión de Apache HTTP Server 2.4.49 (versiones anteriores no se ven afectadas)**

RECOMENDACIONES

Se recomienda a los usuarios del software Apache HTTP Server a realizar la actualización a la versión más reciente para mitigar el problema encontrado.

DICCIONARIO DE DATOS

Ataque de fuerza bruta: Un ataque de fuerza bruta es un procedimiento para averiguar una contraseña que consiste en probar todas las combinaciones posibles hasta encontrar la combinación correcta.
Vulnerabilidad: Debilidad o fallo de un sistema que puede ser aprovechado con fines maliciosos (normalmente mediante un programa que se denomina exploit). Cuando se descubre el desarrollador del software o hardware lo solucionará publicando una actualización de seguridad del producto
Código arbitrario (RCE): Hace referencia, en el campo de la seguridad informática, a la capacidad de un atacante para ejecutar comandos o inyectar código en una aplicación, aprovechando generalmente alguna vulnerabilidad.
CVE: Acrónimo del inglés en Common Vulnerabilities and Exposures; en español, listado de vulnerabilidades de seguridad conocidas, en el que se puede identificar una vulnerabilidad, así como un resumen de las características, efectos, las versiones del software afectadas, posibles soluciones o mitigaciones de dicha vulnerabilidad.
URL: Las siglas URL (Uniform Resource Locator) hacen referencia a la dirección que identifica un contenido colgado en Internet.

REFERENCIAS

1. https://www.tenable.com/cve/CVE-2021-41773
2. https://conciber.gob.gt/?page_id=1208
3. https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-41773
4. https://www.appserv.org/en/
5. https://github.com/iilegacyyii/PoC-CVE-2021-41773
6. https://nvd.nist.gov/vuln/detail/CVE-2021-41773

ÁREA PARA DEFINICIONES