Nro. Alerta:	EC-2022-047	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	15-marzo-2022	**Vulnerabilidades en Apache HTTP Server**	V 1.1

I. DATOS GENERALES:

Clase de alerta: Vulnerabilidad
Tipo de incidente: Sistema y/o Software Abierto
Nivel de riesgo: Alta

II. ALERTA

Diferentes vulnerabilidades fueron encontradas en Apache HTTP Server 2.4, en la versión 2.4.52 y versiones anteriores; la explotación de estas vulnerabilidades podría provocar desbordamiento de búfer, escalada de privilegios o una denegación de servicio.

Figura 1. Logotipo APACHE

III.INTRODUCCIÓN

Apache HTTP Server es un software de servidor web gratuito y de código abierto para plataformas Unix Microsoft Windows, Macintosh y otras, que implementa el protocolo HTTP/1.1; a través de este servidor se ejecutan el 46% de los sitios web de todo el mundo, es mantenido y desarrollado por la Apache Software Foundation.

A continuación, se listan diferentes vulnerabilidades y sus respectivas descripciones; que afectan al Servidor Apache HTTP: 2.4.0 - 2.4.52.

Dirección: Av. Amazonas N40-71 y Gaspar de Villaroel
Código postal: 170501 / Quito-Ecuador
Teléfono: 593-2 2271 180 - www.arcotel.gob.ec

Nro. Alerta:	EC-2022-047	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	15-marzo-2022	**Vulnerabilidades en Apache HTTP Server**	V 1.1

ÍTEM	CVE	DESCRIPCIÓN
1	CVE-2022-23943	La vulnerabilidad de escritura fuera de los límites en mod_sed del servidor Apache HTTP permite a un atacante sobrescribir la memoria del montón con datos posiblemente proporcionados por el atacante.
2	CVE-2022-22721	Si LimitXMLRequestBody está configurado para permitir cuerpos de solicitud de más de 350 MB (el valor predeterminado es 1 M) en sistemas de 32 bits, se produce un desbordamiento de enteros que luego provoca escrituras fuera de los límites.
3	CVE-2022-22720	Apache HTTP Server 2.4.52 y versiones anteriores no pueden cerrar la conexión entrante cuando se encuentran errores al descartar el cuerpo de la solicitud, lo que expone al servidor al contrabando de solicitudes HTTP.
4	CVE-2022-22719	Un cuerpo de solicitud cuidadosamente elaborado puede causar una lectura en un área de memoria aleatoria que podría causar que el proceso se bloquee.

Tabla 1. Vulnerabilidades del servidor Apache HTTP 2.4
Fuente: Apache HTTP Server Project.

IV. VECTOR DE ATAQUE:

El vector de ataque de las vulnerabilidades descritas a continuación es de carácter remoto; a continuación, se menciona un resumen de dichas vulnerabilidades.

ÍTEM	CVE	RESUMEN
1	CVE-2022-23943	La vulnerabilidad permite que en atacante remoto pueda desencadenar una escritura fuera de los límites y ejecutar código arbitrario en el sistema de destino.
2	CVE-2022-22721	La vulnerabilidad permite a un atacante remoto desencadenar la corrupción de la memoria y ejecutar código arbitrario en el sistema de destino.
3	CVE-2022-22720	La vulnerabilidad permite que un atacante remoto realice ataques de contrabando de solicitudes HTTP.
4	CVE-2022-22719	La vulnerabilidad permite que un atacante remoto realice un ataque de denegación de servicio (DoS).

Tabla 2. CVE y resumen de las vulnerabilidades
Fuente: Apache HTTP Server Project.

Dirección: Av. Amazonas N40-71 y Gaspar de Villaroel
Código postal: 170501 / Quito-Ecuador
Teléfono: 593-2 2271 180 - www.arcotel.gob.ec

Nro. Alerta:	EC-2022-047	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	15-marzo-2022	**Vulnerabilidades en Apache HTTP Server**	V 1.1

V. IMPACTO:

La explotación activa de las vulnerabilidades descubiertas provocaría:

- Desbordamiento de búfer.
- Escalada de privilegios.
- Denegación de servicio.

A continuación, se menciona el impacto y la mitigación para cada una de las vulnerabilidades.

ÍTEM	CVE	IMPACTO	MITIGACIÓN
1	CVE-2022-23943	Confidencialidad: En parte Integridad: En parte Disponibilidad: En parte	Upgrade: HTTP Server 2.4.53
2	CVE-2022-22721	Confidencialidad: En parte Integridad: En parte Disponibilidad: En parte	Upgrade: HTTP Server 2.4.53
3	CVE-2022-22720	Confidencialidad: En parte Integridad: En parte Disponibilidad: En parte	Upgrade: HTTP Server 2.4.53
4	CVE-2022-22719	Confidencialidad: Ninguno Integridad: Ninguno Disponibilidad: En parte	Upgrade: HTTP Server 2.4.53

VI. RECOMENDACIONES:

El EcuCert recomienda a su comunidad objetivo:

- Instalar las respectivas actualizaciones entregadas por el proveedor.
- Implementar un plan de respuesta a emergencias de la Organización/Institución.

Dirección: Av. Amazonas N40-71 y Gaspar de Villaroel
Código postal: 170501 / Quito-Ecuador
Teléfono: 593-2 2271 180 - www.arcotel.gob.ec

Nro. Alerta:	EC-2022-047	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	15-marzo-2022	**Vulnerabilidades en Apache HTTP Server**	V 1.1

VII. REFERENCIAS:

Apache. (14 de 03 de 2022). *Apache*. Obtenido de Apache: https://httpd.apache.org/security/vulnerabilities_24.html

HOSTINGER. (23 de 02 de 2022). *HOSTINGER*. Obtenido de HOSTINGER: https://www.hostinger.es/tutoriales/que-es-apache/

VulDB. (14 de 03 de 2022). *VulDB*. Obtenido de VulDB: https://vuldb.com/es/?id.194862

VulDB. (14 de 03 de 2022). *VulDB*. Obtenido de VulDB: https://vuldb.com/es/?id.194860

VulDB. (14 de 03 de 2022). *VulDB*. Obtenido de VulDB: https://vuldb.com/es/?id.194859

VulDB. (14 de 03 de 2022). *VulDB*. Obtenido de VulDB: https://vuldb.com/es/?id.194861