CONCIBER
Comité Nacional de Seguridad Cibernética

ALERTA

Vulnerabilidad de Software

Fecha: **24/10/2022**

Problemática: **Vulnerabilidad de ejecución de código arbitrario en Apache Commons Text**

Correlativo: **AA-0056**

Institución / Sector: **Municipalidad de San Francisco el Alto del Departamento de Totonicapán**

Nivel de priorización

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

Matriz de Evaluación

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

CONTEXTO

El software del Servidor HTTP Apache se ve afectado por una vulnerabilidad identificada como "CVE-2022-42889", que afecta a la funcionalidad "Commons Text" y se encuentra presente en las versiones de este software. La explotación exitosa de esta vulnerabilidad podría llevar a un actor de amenazas a la ejecución de código arbitrario.

SITUACIÓN

De acuerdo a la información obtenida por el Centro Estratégico de Monitoreo – CEM, la vulnerabilidad que existe en el servidor HTTP de Apache, surge a raíz de la implementación insegura de la funcionalidad de interpolación variable de Commons Text. El método StringSubstitutor.createInterpolator() crea un interpolador y permitirá búsquedas de cadenas como se define en StringLookupFactory. Esto se puede usar pasando una cadena " ${prefix:name} " donde el prefijo es la búsqueda mencionada anteriormente. El uso de las búsquedas de "script", "dns" o "url" permitiría que una cadena diseñada ejecute scripts arbitrarios cuando se pasa al objeto interpolador. Lo que permitirá al ciberdelincuente ejecutar código arbitraio en el sistema objetivo.

RECOMENDACIONES

- Esta falla se puede evitar asegurándose de que cualquier entrada externa utilizada con los métodos de búsqueda de Commons-Text se desinfecte adecuadamente. La entrada que no sea de confianza siempre debe desinfectarse a fondo antes de usarla en cualquier situación potencialmente riesgosa.
- Actualizar la versión Apache Commons Text a su úlima versión
- Considere implementar planes de recuperación ante desastres de TI que contengan procedimientos para realizar copias de seguridad de datos periódicas que se puedan usar para restaurar datos de la organización. Asegúrese de que las copias de seguridad se almacenen fuera del sistema y estén protegidas de los métodos comunes que los adversarios pueden usar para obtener acceso y destruir las copias de seguridad para evitar la recuperación

DICCIONARIO DE DATOS

- Atacante (ciberdelincuente, actor de amenazas): Persona que realiza actividades delictivas en la red contra personas o sistemas informáticos, pudiendo provocar daños económicos o reputacionales mediante robo, filtrado de información.
- Defacement: Técnica empleada en la desconfiguración de sitios web
- Código arbitrario: Capacidad de un atacante para ejecutar comandos o inyectar código en una aplicación, aprovechando generalmente alguna vulnerabilidad

REFERENCIAS

1. https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-42889
2. https://access.redhat.com/security/cve/cve-2022-42889

ÁREA PARA DEFINICIONES