Nro. Alerta:	EC-2022-070	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	20-mayo-2022	**Vulnerabilidad presente en Apache Tomcat**	V 1.1

I. DATOS GENERALES:

Clase de alerta: Vulnerabilidad
Tipo de incidente: Sistema vulnerable
Nivel de riesgo: Alta

II. ALERTA

Problema de liberación de recursos en algunas versiones de Apache Tomcat, fue identificado por el equipo de "Apache Tomcat Security", el 21 de diciembre de 2021 y se hizo público el 12 de mayo de 2022, a través del CVE-2022-25762.

Figura 1.- lustración relacionada a Apache Tomcat
Fuente: Hispasec

III. INTRODUCCIÓN

El 12 de mayo de 2022, la Fundación de Software Apache dio a conocer una vulnerabilidad calificada como alta, asociada a Apache Tomcat 8.5.0 a 8.5.75 o Apache Tomcat 9.0.0.M1 a 9.0.20, es posible que la aplicación continúe usando el *socket*[1] después de haberlo cerrado. El manejo de errores que se produce en este caso, podría hacer que un *objeto* se coloque dos veces en el *grupo*. Esto podría dar lugar a que se retornen datos incorrectos o con errores en las conexiones posteriores que utilicen el mismo objeto al mismo tiempo.

[1] Un socket es el conjunto de la dirección IP y el un número de puerto asociado al servicio.

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-2022-070	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	20-mayo-2022	**Vulnerabilidad presente en Apache Tomcat**	V 1.1

IV. VECTOR DE ATAQUE:

Red

V. IMPACTO:

Según análisis realizado por Red Hat en la valoración del CVE-2022-25762, en la Tabla No. 1, a manera referencial se presenta el impacto sobre sus sistemas.

	Sistemas Red Hat
Puntaje base de CVSS v3	8.6
Complejidad de ataque	Bajo
Privilegios requeridos	Ninguno
Interacción con usuario	Ninguna
Impacto a la confidencialidad	Alto
Impacto a la Integridad	Bajo
Impacto a la disponiblidad	Bajo

Tabla No. 1. Impacto del 2022-25762 sobre sistemas Red Hat
Fuente: RedHat

VI. INDICADORES DE COMPROMISO:

VERSIONES AFECTADAS:

Apache Tomcat: 9.0.0.M1 a 9.0.20
Apache Tomcat: 8.5.0 a 8.5.75

VII. RECOMENDACIONES:

El EcuCERT recomienda a su comunidad objetivo, que poseen las versiones Apache Tomcat 8.5.0 a 8.5.75 o Apache Tomcat 9.0.0.M1 a 9.0.20, lo siguiente:

- Actualizar a Apache Tomcat 9.0.21 o posterior.
- Actualice a Apache Tomcat 8.5.76 o posterior.
- Se sugiere revisar de manera periódica, los sitios https://tomcat.apache.org/security-9.html y https://tomcat.apache.org/security-8.html, para conocer vulnerabilidades que afectan a las versiones indicadas.

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-2022-070	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	20-mayo-2022	**Vulnerabilidad presente en Apache Tomcat**	V 1.1

VIII. REFERENCIAS:

- Apache Tomcat. (n.d.). *Apache Tomcat® - Apache Tomcat 8 vulnerabilities*. Apache. https://tomcat.apache.org/security-8.html#Fixed_in_Apache_Tomcat_8.5.76
- Apache Tomcat. (n.d.). *Apache Tomcat® - Apache Tomcat 9 vulnerabilities*. APACHE. https://tomcat.apache.org/security-9.html#Fixed_in_Apache_Tomcat_9.0.21
- CVE. (n.d.). *cve-website*. CVE. https://www.cve.org/CVERecord?id=CVE-2022-25762.
- Hispasec, H. (2018, Octubre 4). *Solucionadas tres vulnerabilidades en servidores apache tomcat*. Hispasec. https://unaaldia.hispasec.com/2016/11/solucionadas-tres-vulnerabilidades-en-servidores-apache-tomcat-2.html.
- Rapid7. (n.d.). *Apache Tomcat: Important: Request mix-up (CVE-2022-25762)*. Rapid7. https://www.rapid7.com/db/vulnerabilities/apache-tomcat-cve-2022-25762/.
- RedHat. (2022, Mayo 11). *Red Hat Customer Portal - Access to 24x7 support and knowledge*. RedHat. https://access.redhat.com/security/cve/cve-2022-25762.
- Thomas, M. (2022, Mayo 12). *Apache*. Obtenido de apache.org: https://lists.apache.org/thread/qzkqh2819x6zsmj7vwdf14ng2fdgckw7.