BOLETÍN DE ALERTA

Boletín Nro.: 2017-12
Fecha de publicación: 19/09/2017
Tema: Vulnerabilidades críticas en Apache Tomcat

Sistemas afectados:

- Apache Tomcat 7.0.0 a 7.0.79

Descripción:

Se ha descubierto dos vulnerabilidades críticas que afectan a Apache Tomcat, un contenedor web con soporte de servlets y JSPs muy utilizado. Las versiones afectadas van desde la 7.0.0 a 7.0.79.

Una de las vulnerabilidades fue identificada como CVE-2017-12615, y se trata de una vulnerabilidad de ejecución de código remoto mediante subida de JSP. En los servidores sobre sistema operativo Windows con HTTP PUTs activo es posible subir un archivo JSP arbitrario al servidor a través de una petición construida especialmente. Esto permite la inyección de cualquier código malicioso que puede ser ejecutado posteriormente por un atacante remoto, como por ejemplo una webshell, backdoor, o similar.

También se ha encontrado una vulnerabilidad que permite a un atacante no autorizado visualizar información, la cual fue identificada como CVE-2017-12616. Cuando se utiliza la clase VirtualDirContext es posible, mediante peticiones construidas especialmente, evadir las restricciones de seguridad y/o visualizar el código fuente JSP de recursos servidor por VirtualDirContext.

Impacto:

Un cibercriminal puede obtener el control total del servidor en el que se ejecuta una versión vulnerable de Apache Tomcat.

Solución:

Las vulnerabilidades fueron corregidas en la versión Apache Tomcat 7.0.81 o posterior. Se recomienda actualizar a dicha versión. Puede descargar la última versión de Apache Tomcat desde el sitio oficial o desde los repositorios oficiales de su distribución de sistema operativo:
https://tomcat.apache.org/download-70.cgi#7.0.81

CERT-PY Equipo de Respuestas ante Emergencias Cibernéticas
Secretaría Nacional de Tecnologías de la Información y Comunicación (SENATICs)
Gral. Santos y Concordia – Complejo Santos – Ofic. E14
cert@cert.gov.py | +595 21 201014 | +595 21 3276902
Asunción - Paraguay | www.cert.gov.py
@CERTpy
/CERT-Py

Información adicional:

http://mail-archives.us.apache.org/mod_mbox/www-announce/201709.mbox/%3cde541c4a-55b1-a4d3-4fbe-f8e3800b920f@apache.org%3e

http://mail-archives.us.apache.org/mod_mbox/www-announce/201709.mbox/%3c16df1f59-ea31-0789-f0c8-5432c60de8fc@apache.org%3e

CERT-PY Equipo de Respuestas ante Emergencias Cibernéticas
Secretaría Nacional de Tecnologías de la Información y Comunicación (SENATICs)
Gral. Santos y Concordia – Complejo Santos – Ofic. E14
cert@cert.gov.py | +595 21 201014 | +595 21 3276902
Asunción - Paraguay | www.cert.gov.py

@CERTpy
/CERT-Py