Para ti que tu servidor web es Apache Tomcat, debes instalar inmediatamente la última versión disponible de la aplicación del servidor para evitar que los hackers tomen control no autorizado sobre ella.

Esto se sabe que es posible, ya que todas las versiones (9.x / 8.x / 7.x / 6.x) del Apache Tomcat lanzado en los últimos 13 años se han encontrado vulnerables a un nuevo archivo de alta gravedad (CVSS 9.8) error de lectura e inclusión, que puede explotarse en la configuración predeterminada.

Sin embargo, es preocupante, decir que varias vulnerabilidades de prueba de concepto (1, 2, 3, 4 y más) han aparecido en Internet, lo que facilita que cualquiera pueda hackear servidores web vulnerables de acceso público.

Apodado 'Ghostcat' y rastreado como CVE-2020-1938, la falla podría permitir que los atacantes remotos no autenticados lean el contenido de cualquier archivo en un servidor web vulnerable y obtengan archivos de configuración confidenciales.

Pero…

¿Qué es la a falla de Ghostcat y cómo funciona?

La vulnerabilidad reside en el protocolo AJP del software Apache Tomcat que surge debido al manejo inadecuado de un atributo.

Si el sitio permite a los usuarios cargar archivos, un atacante puede cargar primero un archivo que contenga código de script JSP malicioso en el servidor (el archivo cargado en sí mismo puede ser de cualquier tipo de archivo, como imágenes, archivos de texto plano, etc.), y luego incluir el archivo cargado explotando el Ghostcat, que finalmente puede resultar en la ejecución remota de código

El protocolo Apache JServ Protocol (AJP) es básicamente una versión optimizada del protocolo HTTP para permitir que Tomcat se comunique con un servidor web Apache.

Aunque el protocolo AJP viene habilitado de forma predeterminada y escucha en el puerto TCP 8009, está vinculado a la dirección IP 0.0.0.0 y solo puede explotarse de forma remota cuando sea accesible para clientes no confiables.

Los investigadores de Chaitin encontraron e informaron este defecto el mes pasado al proyecto Apache Tomcat, que ahora lanzó las versiones Apache Tomcat 9.0.31, 8.5.51 y 7.0.100 para solucionar el problema.

Se recomienda encarecidamente a los administradores web que apliquen las actualizaciones de software lo antes posible y se les aconseja que nunca expongan el puerto AJP a clientes que no son de confianza porque se comunican a través del canal inseguro y deben usarse dentro de una red confiable.