Alerta de seguridad cibernética	9VSA21-00380-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	02 de febrero de 2021
Última revisión	02 de febrero de 2021

NOTIFICACIÓN

La información consignada en el presente informe es producto del análisis de múltiples fuentes, de terceras partes, del propio fabricante e investigación propia del equipo CSIRT. La información contenida en los informes o comunicados está afecta a actualizaciones.

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT de Gobierno, comparte la información entregada por Apache, sobre vulnerabilidades que afectan a su producto Apache Shiro.

Este informe incluye las medidas de mitigación, consistentes en implementar medidas recomendadas por el proveedor e instalar las actualizaciones de los productos afectados cuando estén disponibles.

Vulnerabilidad

CVE-2020-17523

Impacto

La vulnerabilidad permite a un atacante remoto evadir procesos de autenticación enviando una solicitud HTTP especialmente diseñada, lo que le permitiría ganar acceso no autorizado a la aplicación.

CVE-2020-17523 existe debido a un error al procesar solicitudes de autenticación en Apache Shiro con Spring.

Productos afectados

Apache Shiro, versiones de la 1.0.0. a la 1.7.0.

Mitigación

Instalar las correspondientes actualizaciones desde el sitio del proveedor.

Enlaces

http://shiro.apache.org/documentation.html#current-release

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-17523