Alerta de Seguridad Cibernética

Alerta de seguridad cibernética	9VSA21-00390-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Crítico
TLP	Blanco
Fecha de lanzamiento original	11 de febrero de 2021
Última revisión	11 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, comparte la información entregada por SAP sobre una vulnerabilidad crítica que afecta a su producto SAP Commerce.

Este informe incluye las medidas de mitigación, consistentes en instalar las últimas actualizaciones de los productos afectados.

Vulnerabilidad

CVE-2021-21477

Impacto

CVE-2021-21477 es una vulnerabilidad crítica que permite a ciertos usuarios “con los privilegios requeridos” editar las reglas de Drools, un motor que crea las reglas para SAP Commerce. Debido a un error de configuración de los permisos de usuario por defecto con que se entrega SAP Commerce, usuarios de bajos privilegios y grupos de usuarios tienen permiso para cambiar el atributo ruleContent en Drools y ganar acceso no deseado.

Esto permite a un atacante con bajos privilegios inyectar código malicioso a los scripts de reglas de Drools, permitiéndole vulnerar la confidencialidad, integridad y disponibilidad de la aplicación.

Productos Afectados

SAP Commerce versiones 1808, 1811, 1905, 2005 y 2011.

Mitigación

Instalar las respectivas actualizaciones desde el sitio del proveedor.

Enlaces

https://support.sap.com/en/my-support/knowledge-base/security-notes-news.html
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21477

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2021.02.11 12:06:29 -03'00'