

Alerta de seguridad cibernética	9VSA22-00734-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	25 de octubre de 2022
Última revisión	25 de octubre de 2022

## 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 CSIRT de Gobierno. La información contenida en los informes o comunicados está afectada a actualizaciones.

## Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT de Gobierno, comparte información sobre dos vulnerabilidades dadas a conocer y que afectan a Atlassian Jira Align.

## Vulnerabilidades

CVE-2022-36802  
CVE-2022-36803

## Impacto

### Vulnerabilidades de riesgo alto

CVE-2022-36802: Una vulnerabilidad es del tipo server-side request forgery (SSRF) en la configuración de Connectors, lo que permite a un usuario obtener credenciales de una cuenta de servicio Atlassian.

CVE-2022-36803: Controles de Autorización Insuficientes en "People" permiten que cualquier usuario con estos permisos modifique su propio rol al de Super Admin.

### Productos afectados

Atlassian Jira Align 10.107.4

### Mitigación

Actualizar a la versión 10.109.3 o más nueva.

### Enlaces

<https://bishopfox.com/blog/jira-align-advisory>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-36802>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-36803>