

Alerta de seguridad cibernética	9VSA21-00501-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Crítica
TLP	Blanco
Fecha de lanzamiento original	04 de octubre de 2021
Última revisión	04 de octubre 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 afectada a actualizaciones.

## Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática del Gobierno de Chile, CSIRT de Gobierno, comparte información relacionada con una vulnerabilidad crítica que afecta a IBM QRadar.

Este informe incluye las medidas de mitigación, consistentes en instalar la última actualización de los productos afectados.

## Vulnerabilidad

CVE-2021-37967

## Impactos

IBM QRadar Azure marketplace images include la Open Management RPM, vulnerable a CVE-2021-38647.

Explotar CVE-2021-38647 permite a un atacante remoto ejecutar código arbitrario en el sistema.

### Productos Afectados

IBM QRadar Azure marketplace images 7.3.0 a 7.3.3 Patch 9

IBM QRadar Azure marketplace images 7.4.0 a 7.4.3 Patch 2

### Mitigación

Instalar las respectivas actualizaciones entregadas por el proveedor.

## Enlaces

<https://www.ibm.com/support/pages/security-bulletin-ibm-qradar-azure-marketplace-images-include-open-management-infrastructure-rpm-which-vulnerable-remote-code-execution-cve-2021-38647>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-38647>