Alerta de seguridad cibernética	9VSA24-00959-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
TLP	Blanco
Fecha de lanzamiento original	18 de enero de 2024
Última revisión	18 de enero de 2024

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 afecta a actualizaciones.

Resumen

El CSIRT de Gobierno comparte información de vulnerabilidades que afectan a Aria Automation de VMware (antes llamado vRealize Automation).

Vulnerabilidades

CVE-2023-34063

Impacto

Vulnerabilidad de riesgo crítico:

CVE-2023-34063: Vulnerabilidad Missing Access Control en Aria Automation, que puede llevar a un acceso a organizaciones y workflows remotos. CVSS: 9.9.

Mitigación

Actualizar según:
VMware Aria Automation: https://kb.vmware.com/s/article/96098
VMware Cloud Foundation (Aria Automation) 5.x, 4.x: https://kb.vmware.com/s/article/96136

Productos afectados

VMware Aria Automation (antes vRealize Automation): 8.11.x, 8.12.x, 8.13.x y 8.14.x.
VMware Cloud Foundation (Aria Automation) 4.x y 5.x.

Enlaces

https://www.vmware.com/security/advisories/VMSA-2024-0001.html

CSIRT Gobierno de Chile
Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2024.01.19 11:35:27 -03'00'