

Alerta de Seguridad Cibernética

Equipo de Respuesta ante Incidentes de Seguridad Informática | CSIRT de Gobierno
Ministerio del Interior y Seguridad Pública
Subsecretaría del Interior

Alerta de seguridad cibernética	9VSA23-00797-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Crítico
TLP	Blanco
Fecha de lanzamiento original	3 de marzo de 2023
Última revisión	3 de marzo de 2023

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 Equipo de Respuesta ante Incidentes de Seguridad Informática del Gobierno de Chile, CSIRT de Gobierno, comparte información sobre vulnerabilidades críticas en ArubaOS.

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

Vulnerabilidad

CVE-2023-22747
CVE-2023-22748
CVE-2023-22749
CVE-2023-22750
CVE-2023-22751
CVE-2023-22752

Impacto

CVE-2023-22747, CVE-2023-22748, CVE-2023-22749 y CVE-2023-22750: Un atacante remoto no autenticado puede aprovecharlos enviando paquetes especialmente diseñados al PAPI, a través del puerto UDP 8211, lo que resulta en la ejecución de código arbitrario como usuario privilegiado en ArubaOS.

CVE-2023-22751 y CVE-2023-22752: Estas fallas se pueden explotar mediante el envío de paquetes especialmente diseñados al PAPI a través del puerto UDP 8211, lo que permite a atacantes remotos no autenticados ejecutar código arbitrario como usuarios privilegiados en ArubaOS.

Productos afectados

ArubaOS 8.6.0.19 y anteriores
ArubaOS 8.10.0.4 y anteriores
ArubaOS 10.3.1.0 y anteriores
SD-WAN 8.7.0.0-2.3.0.8 y anteriores

Mitigación

Instalar las respectivas actualizaciones entregadas por el proveedor.

Enlaces

<https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-22747>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-22748>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-22749>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-22750>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-22751>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-22752>