Alerta de seguridad cibernética	9VSA24-00978-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
TLP	Blanco
Fecha de lanzamiento original	21 de febrero de 2024
Última revisión	21 de febrero 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 sobre vulnerabilidad que afecta al complemento de autenticación mejorada (EAP) de VMware.

Vulnerabilidades

CVE-2024-22245
CVE-2024-22250

Impacto

Vulnerabilidades críticas

CVE-2024-22245: El complemento de autenticación mejorada (EAP) de VMware contiene una vulnerabilidad de retransmisión de autenticación arbitraria.

CVE-2024-22250: El complemento de autenticación mejorada (EAP) de VMware contiene una vulnerabilidad de secuestro de sesión.

Mitigación

Para abordar CVE-2024-22245 y CVE-2024-22250, elimine el complemento EAP siguiendo las instrucciones del proveedor: https://www.vmware.com/security/advisories/VMSA-2024-0003.html

Productos afectados

Complemento de autenticación mejorada (EAP) de VMware.

Enlaces

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-22245
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-22250

CSIRT Gobierno de Chile
Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2024.02.21 15:54:49 -03'00'