Alerta de Seguridad Cibernética

Alerta de seguridad cibernética	9VSA22-00736-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Crítico
TLP	Blanco
Fecha de lanzamiento original	27 de octubre de 2022
Última revisión	27 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 afecta a actualizaciones.

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT de Gobierno, comparte información sobre vulnerabilidades, incluida una crítica, parchadas por VMware.

Vulnerabilidades

CVE-2021-39144 CVE-2022-31678

Impacto

Vulnerabilidades críticas
CVE-2021-39144: Un atacante malicioso podría lograr ejecución remota de código en el contexto de "root" en la appliance, debido a un endpoint no autenticado en VMware Cloud Foundation (NSX-V).

Productos afectados
VMware Cloud Foundation y VMware Cloud Foundation (NSX-V).

Mitigación
Instalar las respectivas actualizaciones entregadas por el proveedor.

Enlaces
https://www.vmware.com/security/advisories/VMSA-2022-0027.html
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-39144
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-31678

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2022.10.27 15:07:55 -03'00'