Alerta de seguridad cibernética	9VSA22-00608-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Crítico
TLP	Blanco
Fecha de lanzamiento original	5 de abril de 2022
Última revisión	5 de abril 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 del Gobierno de Chile, CSIRT de Gobierno, comparte información sobre nuevas vulnerabilidades en productos de VMware.

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

Vulnerabilidades

CVE-2022-22965
CVE-2022-22948
CVE-2022-22943
CVE-2022-22951
CVE-2022-22952
CVE-2022-22943
CVE-2022-22944
CVE-2022-22945

Impacto

Vulnerabilidades críticas e importantes

CVE-2022-22965: Conocida como Spring4Shell, esta vulnerabilidad crítica permite a un atacante remoto ejecutar código arbitrario en el sistema objetivo. La vulnerabilidad existe debido a una inapropiada validación de inputs. La explotación exitosa de esta vulnerabilidad puede resultar en un compromiso total de un sistema vulnerable.

Descrita previamente por el CSIRT de Gobierno aquí: csirt.gob.cl/vulnerabilidades/9vsa22-00605-01/

CVE-2022-22951: Vulnerabilidad de inyección de comandos OS en VMware Carbon Black App Control (AppC). Un actor malicioso autenticado y con altos privilegios, con acceso de red a la interfaz de administración de VMware App Control podría ejecutar comandos en el servidor, debido a una validación inapropiada de imputs, llevando a la ejecución remota de código.

CVE-2022-22952: Vulnerabilidad de carga de archivos en VMware Carbon Black App Control, que permite a un actor malicioso con acceso administrativo a la interfaz de control de VMware App Control ejecutar código en una instancia Windows en la que AppC Server esté instalado, a través de la carga de un archivo especialmente diseñado.

CVE-2022-22945: Vulnerabilidad de inyección de shell CLI que afecta a VMware NSX Data Center for vSphere. Un actor malicioso con acceso SSH a una aplicación NSX-Edge (NSX-V) puede ejecutar comandos arbitrarios en el sistema operativo como root.

Productos afectados

CVE-2022-22965
Tanzu Application Service: https://network.pivotal.io/products/elastic-runtime/
Tanzu Operations Manager: https://network.tanzu.vmware.com/products/ops-manager
VMware TKGI: https://network.pivotal.io/products/pivotal-container-service/

CVE-2022-22948
VMware vCenter Server (vCenter Server)
VMware Cloud Foundation (Cloud Foundation)

CVE-2022-22951 y CVE-2022-22952
VMware Carbon Black App Control (AppC)

CVE-2022-22943
VMware Tools for Windows

CVE-2022-22944
VMware Workspace ONE Boxer

CVE-2022-22945
VMware NSX Data Center for vSphere.
VMware Cloud Foundation (Cloud Foundation)

Mitigación
Instalar las respectivas actualizaciones entregadas por el proveedor.

Enlaces
https://www.vmware.com/security/advisories/VMSA-2022-0010.html
https://www.vmware.com/security/advisories/VMSA-2022-0009.html

https://www.vmware.com/security/advisories/VMSA-2022-0008.html
https://www.vmware.com/security/advisories/VMSA-2022-0007.html
https://www.vmware.com/security/advisories/VMSA-2022-0006.html
https://www.vmware.com/security/advisories/VMSA-2022-0005.html
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22965
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22948
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22943
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22951
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22952
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22943
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22944
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22945

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2022.04.05 12:07:42 -04'00'