VULNERABILIDAD CRÍTICA EN PRODUCTOS VMWARE (06/AGOSTO/2021)

Vulnerabilidades críticas en varios productos de VMware permitirían que atacantes de manera remota puedan acceder a información confidencial

VMware es una herramienta muy popular respecto a las necesidades de optimizar los recursos disponibles, así como la centralización de infraestructura tecnológica de información y comunicación. La posibilidad de contar con varias máquinas virtuales, diferentes sistemas operativos y por lo tanto varios servicios y aplicaciones, ha hecho que en los últimos años esta herramienta de virtualización esté presente en el despliegue de infraestructura IT.

Un problema detectado en los módulos Workspace One Access y Manager Identity permitiría que sin mecanismos de autenticación se pueda acceder a elementos de configuración que eventualmente facilitaría el acceso a un servidor virtualizado. Adicionalmente, se habría detectado una interfaz de acceso y administración expuesta a la red de Internet, por lo cual sujeta a ataques de fuerza bruta.

En consideración al alto riesgo contra la confidencialidad, integridad y disponibilidad de los activos de información administrados por la herramienta VMware, el EcuCERT recomienda a su comunidad objetivo, tomar en consideración las siguientes recomendaciones:

1. Aplicar los parches de actualización y mecanismos de contención emitidos por el desarrollador.
2. Ejecutar aplicaciones con perfiles de usuario con el menor privilegio posible.
3. Implementar mecanismos de monitoreo y control de tráfico enfocados en conexiones atípicas.

Referencias

VMWARE. 2021. HW-137959: VMSA-2021-0016 for vRealize Automation 7.6 (CVE-2021-22002, CVE-2021-22003) (85255). Disponible en https://www.wordfence.com/blog/2021/06/critical-0-day-infancy-product-designer-under-active-attack/

VMWARE. 2021. VMSA-2021-0016. Disponible en https://www.vmware.com/security/advisories/VMSA-2021-0016.html

CVE. 2021. CVE-2021-22002. Disponible en https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-22002

CVE. 2021. CVE-2021-22003. Disponible en https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-22003