BEACON LAB
C S I R T

CYBOLT
Security Innovation

Boletín de Alerta

Boletín Nro.: 2024-36
Fecha de publicación: 18/09/2024
Tema: Vulnerabilidad Crítica en VMware CVE-2024-38812
Traffic Light Protocol (TLP): White

Producto(s) afectado:

- Servidor VMware vCenter
- Fundación VMware Cloud

Descripción

Se ha identificado una vulnerabilidad crítica en la plataforma vCenter Server de VMware, conocida como **CVE-2024-38812**, reportada por los investigadores de TZL durante el concurso de piratería **Matrix Cup 2024** en China. Esta vulnerabilidad, con una puntuación de gravedad **CVSS 9.8**, se debe a un desbordamiento de pila en la implementación del protocolo **DCE/RPC** en vCenter Server, lo que permite la ejecución de código remoto mediante paquetes especialmente diseñados. Los atacantes con acceso a la red podrían comprometer por completo el entorno de vCenter, afectando gravemente la infraestructura virtualizada de las organizaciones.

Adicionalmente, se reporta la **CVE-2024-38813**, una vulnerabilidad que facilita la **escalada de privilegios a root**. Ambas vulnerabilidades representan un riesgo severo para la seguridad empresarial, dado que permiten tanto la ejecución remota de código como la elevación de privilegios.

Se recomienda encarecidamente aplicar las actualizaciones de seguridad proporcionadas por VMware de manera inmediata para mitigar estos riesgos y evitar compromisos en los sistemas.

Estas fallas requieren atención urgente para evitar incidentes de seguridad que puedan comprometer entornos críticos.

Solución

El proveedor exploró alternativas para mitigar la vulnerabilidad dentro del producto, sin embargo, tras un análisis exhaustivo, se concluyó que estas soluciones no eran viables. La única forma efectiva de resolver esta vulnerabilidad es aplicar la actualización recomendada en el CVE correspondiente, se puede ver en la columna de Fixed versión.

VMware Product	Version	Running On	CVE	CVSSv3	Severity	Fixed Version	Workarounds	Additional Documentation
vCenter Server	8.0	Any	CVE-2024-38812, CVE-2024-38813	9.8, 7.5	Critical	8.0 U3b	None	FAQ
vCenter Server	7.0	Any	CVE-2024-38812, CVE-2024-38813	9.8, 7.5	Critical	7.0 U3s	None	FAQ
VMware Cloud Foundation	5.x	Any	CVE-2024-38812, CVE-2024-38813	9.8, 7.5	Critical	Async patch to 8.0 U3b	None	Async Patching Guide: KB88287
VMware Cloud Foundation	4.x	Any	CVE-2024-38812, CVE-2024-38813	9.8, 7.5	Critical	Async patch to 7.0 U3s	None	Async Patching Guide: KB88287

https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/24968

Información adicional:

- https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/24968
- https://www.bleepingcomputer.com/news/security/broadcom-fixes-critical-rce-bug-in-vmware-vcenter-server/
- https://securityonline.info/cve-2024-38812-vmwares-9-8-severity-security-nightmare/
- https://nvd.nist.gov/vuln/detail/CVE-2024-38812

BEACON LAB

C S I R T

CYBOLT

Security Innovation

info@beaconlab.mx

beaconlab.mx

contact@cybolt.com

cybolt.com