Broadcom lanzó el martes actualizaciones para solucionar una vulnerabilidad crítica en VMware vCenter Server que podría permitir la ejecución remota de código.

La vulnerabilidad, identificada como CVE-2024-38812 (con una puntuación CVSS de 9.8), se clasifica como un desbordamiento de memoria en el protocolo DCE/RPC.

> *«Un atacante con acceso a la red de vCenter Server puede activar esta vulnerabilidad al enviar un paquete de red especialmente manipulado, lo que podría conducir a la ejecución remota de código,»* informó el proveedor de servicios de virtualización en un boletín.

Este problema es similar a otras dos vulnerabilidades de ejecución remota de código, CVE-2024-37079 y CVE-2024-37080 (con puntuaciones CVSS de 9.8), que VMware corrigió en vCenter Server en junio de 2024.

Además, VMware ha abordado una vulnerabilidad de escalada de privilegios en vCenter Server (CVE-2024-38813, puntuación CVSS: 7.5) que podría permitir a un atacante con acceso a la red de la instancia elevar sus privilegios a root mediante el envío de un paquete de red especialmente diseñado.

Los investigadores de seguridad zbl y srs del equipo TZL han sido reconocidos por descubrir e informar sobre estas vulnerabilidades durante la competencia de ciberseguridad Matrix Cup celebrada en China en junio de 2024. Las vulnerabilidades se han corregido en las siguientes versiones:

- vCenter Server 8.0 (Corregido en 8.0 U3b)
- vCenter Server 7.0 (Corregido en 7.0 U3s)
- VMware Cloud Foundation 5.x (Corregido en 8.0 U3b como un parche asíncrono)
- VMware Cloud Foundation 4.x (Corregido en 7.0 U3s como un parche asíncrono)

Broadcom indicó que no tiene conocimiento de explotación maliciosa de estas

vulnerabilidades, pero ha recomendado a los clientes actualizar sus instalaciones a las versiones más recientes para protegerse contra posibles amenazas.

> *«Estas vulnerabilidades están relacionadas con la gestión y corrupción de memoria, y pueden ser utilizadas contra los servicios de VMware vCenter, permitiendo potencialmente la ejecución remota de código,»* explicó la empresa.

Este anuncio llega en un momento en que la Agencia de Seguridad Cibernética e Infraestructura de EE.UU. (CISA) y el Buró Federal de Investigaciones (FBI) publicaron un aviso conjunto instando a las organizaciones a eliminar vulnerabilidades de scripting entre sitios (XSS) que los actores de amenazas podrían explotar para comprometer sistemas.

> *«Las vulnerabilidades de scripting entre sitios ocurren cuando los fabricantes no validan, sanitizan o escapan adecuadamente las entradas. Estas fallas permiten a los atacantes inyectar scripts maliciosos en aplicaciones web, lo que puede ser utilizado para manipular, robar o malversar datos en diferentes contextos»*, dijeron las agencias gubernamentales.