La Agencia de Seguridad de Infraestructura y Ciberseguridad de Estados Unidos (CISA) incorporó el viernes a su catálogo de Vulnerabilidades Conocidas Explotadas (KEV) una falla crítica de seguridad que afecta a Broadcom VMware vCenter Server y que fue corregida en junio de 2024, tras confirmar evidencias de explotación activa en entornos reales.

La vulnerabilidad señalada corresponde a CVE-2024-37079 (con una puntuación CVSS de 9.8) y se trata de un desbordamiento de memoria en el heap dentro de la implementación del protocolo DCE/RPC. Este fallo podría permitir que un atacante con acceso a la red del vCenter Server ejecute código de forma remota mediante el envío de un paquete de red especialmente diseñado.

Broadcom solucionó este problema en junio de 2024, junto con CVE-2024-37080, otra vulnerabilidad de tipo heap overflow en la implementación del protocolo DCE/RPC que también podría derivar en ejecución remota de código. Los investigadores Hao Zheng y Zibo Li, de la empresa china de ciberseguridad QiAnXin LegendSec, fueron reconocidos por descubrir y reportar estas fallas.

Durante una presentación en la conferencia de seguridad Black Hat Asia realizada en abril de 2025, los investigadores explicaron que ambas vulnerabilidades forman parte de un conjunto de cuatro fallos detectados en el servicio DCE/RPC: tres desbordamientos de heap y una vulnerabilidad de escalamiento de privilegios. Las otras dos fallas, CVE-2024-38812 y CVE-2024-38813, fueron corregidas por Broadcom en septiembre de 2024.

En particular, los expertos identificaron que uno de los desbordamientos de heap podía encadenarse con la vulnerabilidad de escalamiento de privilegios (CVE-2024-38813) para lograr acceso remoto no autorizado como usuario root y, finalmente, tomar control del entorno ESXi.

Actualmente no se conoce con certeza cómo está siendo explotada CVE-2024-37079, si los ataques están vinculados a algún actor o grupo de amenazas conocido, ni el alcance real de estas actividades. No obstante, Broadcom actualizó su aviso de seguridad para confirmar oficialmente que la vulnerabilidad está siendo explotada en escenarios reales.

“Broadcom cuenta con información que sugiere que la explotación de CVE-2024-37079 ha ocurrido en entornos reales”, indicó la compañía en su actualización.

Ante la existencia de explotación activa, las agencias del Poder Ejecutivo Civil Federal (FCEB) están obligadas a actualizar a la versión más reciente antes del 13 de febrero de 2026, con el fin de garantizar una protección óptima.