Vulnerabilidades de seguridad corregidas recientemente en Progress Kemp LoadMaster y VMware vCenter Server están siendo activamente explotadas, según reportes recientes.

La Agencia de Ciberseguridad e Infraestructura de los EE. UU. (CISA, por sus siglas en inglés) añadió el lunes la vulnerabilidad CVE-2024-1212 (con una puntuación CVSS de 10.0) a su catálogo de Vulnerabilidades Conocidas Explotadas (KEV). Este fallo crítico, detectado en Progress Kemp LoadMaster, fue resuelto por Progress Software en febrero de 2024.

> Según la agencia, *«Progress Kemp LoadMaster presenta una vulnerabilidad de inyección de comandos en el sistema operativo, lo que permite a un atacante remoto y no autenticado acceder al sistema mediante la interfaz de administración de LoadMaster. Esto habilita la ejecución de comandos arbitrarios en el sistema».*

Rhino Security Labs, el equipo que descubrió y notificó esta falla, explicó que, si un atacante obtiene acceso a la interfaz web de administración, puede ejecutar comandos en el sistema, logrando control total sobre el balanceador de carga.

Además, CISA destacó un aviso de Broadcom, alertando sobre la explotación activa de dos vulnerabilidades en VMware vCenter Server. Estas fallas, demostradas durante la competencia de ciberseguridad Matrix Cup en China a principios de año, son:

- CVE-2024-38812 (CVSS: 9.8): Una vulnerabilidad de desbordamiento de memoria en el protocolo DCERPC que podría permitir a un atacante con acceso a la red ejecutar código de forma remota.
- CVE-2024-38813 (CVSS: 7.5): Una falla de escalamiento de privilegios que podría permitir a un atacante con acceso a la red obtener privilegios de administrador root.

Ambas vulnerabilidades fueron solucionadas inicialmente en septiembre de 2024. Sin embargo, el parche para CVE-2024-38812 fue revisado y actualizado nuevamente el mes pasado, ya que los arreglos previos no abordaron completamente el problema.

Aunque los detalles sobre los ataques reales que explotan estas vulnerabilidades aún no han sido revelados, CISA ha instado a las agencias de la Rama Ejecutiva Civil Federal (FCEB) a corregir CVE-2024-1212 antes del 9 de diciembre de 2024, como medida para proteger sus sistemas.

Esta advertencia llega poco después de que Sophos informara sobre el uso activo de una vulnerabilidad crítica en Veeam Backup & Replication (CVE-2024-40711, CVSS: 9.8) por parte de cibercriminales, quienes están distribuyendo un nuevo ransomware denominado Frag.