VMware lanza parches para varias vulnerabilidades que afectan a distintos productos

Autor: I. Stepanenko

Fecha: Sunday 7th of August 2022 06:59:35 PM

El proveedor de servicios de virtualización VMware envió el martes actualizaciones para abordar 10 vulnerabilidades de seguridad que afectan a múltiples productos y que podrían ser abusados por atacantes no autenticados para realizar acciones maliciosas.

Los problemas, rastreados desde CVE-2022-31656 hasta CVE-2022-31665 (puntuación CVSS: 4.7 a 9.8), afectan a VMware Workspace ONE Access, Workspace ONE Access Connector, Identity Manager, Identity Manager Connector, vRealize Automation, Cloud Foundation y el Administrador de Ciclo de Vida de vRealize Suite.

La más grave de las vulnerabilidades es CVE-2022-31656 (puntaje CVSS: 9.8), una falla de omisión de autenticación que afecta a los usuarios del dominio local y que podría ser aprovechada por un mal actor con acceso a la red para obtener derechos administrativos.

VMware también resolvió tres vulnerabilidades de ejecución remota de código

(CVE-2022-31658, CVE-2022-31659 y CVE-2022-31665) relacionadas con la inyección de JDBC y SQL que podría utilizar un adversario con accedo de administrador y de red.

CVE Identifier	CVSSv3	Severity
CVE-2022-31656	9.8	Critical
CVE-2022-31658	8.0	Important
CVE-2022-31659	8.0	Important
CVE-2022-31660, CVE-2022-31661	7.8	Important
CVE-2022-31664	7.8	Important
CVE-2022-31665	7.6	Important
CVE-2022-31657	5.9	Moderate
CVE-2022-31662	5.3	Moderate
CVE-2022-31663	4.7	Moderate

También se corrigió una vulnerabilidad de secuencias de comandos en sitios cruzados (XSS) reflejada (CVE-2022-31663) que, según dijo la compañía, es el resultado de una desinfección inadecuada del usuario, lo que podría conducir a la activación de código JavaScript malicioso.

Para redondear los parches, existen tres errores de escalada de privilegios locales

(CVE-2022-31660, CVE-2022-31661 y CVE-2022-31664) que permiten a un atacante con acceso local escalar privilegios a *«root»,* una vulnerabilidad de inyección de URL (CVE-2022-31657) y un error de recorrido de ruta (CVE-2022-31662).

Aunque la explotación exitosa de CVE-2022-31657 hace posible redirigir a un usuario autenticado a un dominio arbitrario, CVE-2022-31662 podría equipar a un atacante para leer archivos de forma no autorizada.

VMware dijo que no está al tanto de la explotación de estas vulnerabilidades en la naturaleza, pero instó a los clientes que utilizan los productos vulnerables a aplicar los parches inmediatamente para mitigar las amenazas potenciales.