VMware lanzó actualizaciones de seguridad para corregir ocho vulnerabilidades que abarcan sus productos, algunas de las cuales podrían explotarse para lanzar ataques de ejecución remota de código.

Con un seguimiento desde CVE-2022-22954 hasta CVE-2022-22961, con puntuación CVSS de 5.3 a 9.8, los problemas afectan a VMware Workspace ONE Access, VMware Identity Manager, VMware vRealize Automation, VMware Cloud Foundation y vRealize Suite Lifecycle Manager.

Cinco de las ocho vulnerabilidades se califican como críticas, dos como importantes y una como moderada en gravedad. Steven Seeley, del Instituto de Investigación de Vulnerabilidades Qihoo 360, tiene el crédito por informar sobre todas las vulnerabilidades.

Las vulnerabilidades se detallan en la siguiente lista:

- CVE-2022-22954 (puntuación CVSS: 9.8): Vulnerabilidad de ejecución remota de código de inyección de plantilla del lado del servidor, que afecta a VMware Workspace ONE Access e Identity Manager.
- CVE-2022-22955 y CVE-2022-22956 (puntuación CVSS: 9.8): Vulnerabilidades de omisión de autenticación OAuth2 ACS en VMware Workspace ONE Access.
- CVE-2022-22957 y CVE-2022-22958 (puntuación CVSS: 9.1): Vulnerabilidades de ejecución remota de código de inyección JDBC en VMware Workspace ONE Access, Identity Manager y vRealize Automation.
- CVE-2022-22959 (puntuación CVSS: 8.8): Vulnerabilidad de falsificación de solicitud entre sitios (CSRF) en VMware Worspace ONE Access, Identity Manager y vRealize Automation.
- CVE-2022-22960 (puntuación CVSS: 7.8): Vulnerabilidad de escalada de privilegios locales en VMware Workspace ONE Access, Identity Manager y vRealize Automation.
- CVE-2022-22961 (puntuación CVSS: 5.3): Vulnerabilidad de divulgación de información que afecta a VMware Workspace ONE Access, Identity Manager y vRealize Automation.

La explotación exitosa de las vulnerabilidades mencionadas podría permitir que un atacante

aumente los privilegios al usuario raíz, obtenga acceso a los nombres de host de los sistemas de destino y ejecute de forma remota código arbitrario, lo que permitiría una toma de control total.

> *«esta vulnerabilidad crítica debe repararse o mitigarse de inmediato. Las ramificaciones de esta vulnerabilidad son graves»,* dijo VMware.

Aunque la compañía dijo que no ha visto ninguna evidencia de que las vulnerabilidades hayan sido explotadas en la naturaleza, se recomienda aplicar los parches para eliminar las amenazas potenciales.

> *«Las soluciones alternativas, si bien son convenientes, no eliminan las vulnerabilidades y pueden introducir complejidades adicionales que los parches no introducirían»,* dijo la compañía.