Ivanti ha anunciado que una vulnerabilidad crítica de seguridad que afecta a Cloud Service Appliance (CSA) está siendo explotada activamente.

La nueva vulnerabilidad, conocida como CVE-2024-8963, tiene un puntaje CVSS de 9.4 sobre un máximo de 10.0. La empresa la *«abordó incidentalmente»* en el parche 519 de CSA 4.6 y en CSA 5.0.

> *«La vulnerabilidad de Path Traversal en Ivanti CSA antes del parche 519 de la versión 4.6 permite a un atacante remoto no autenticado acceder a funciones restringidas»*, declaró la compañía en un boletín el jueves.

Además, se señaló que esta falla podría ser combinada con CVE-2024-8190 (puntaje CVSS: 7.2), lo que permitiría a un atacante eludir la autenticación de administrador y ejecutar comandos arbitrarios en el dispositivo.

Ivanti también advirtió que tiene conocimiento de un número limitado de clientes que han sido afectados por esta vulnerabilidad, pocos días después de haber informado sobre intentos de explotación dirigidos a CVE-2024-8190.

Esto sugiere que los actores de amenazas están utilizando ambas vulnerabilidades para lograr la ejecución de código en dispositivos vulnerables.

Este avance ha llevado a la Agencia de Ciberseguridad y Seguridad de Infraestructura de EE. UU. (CISA) a incluir la vulnerabilidad en su catálogo de Vulnerabilidades Conocidas Explotadas (KEV), exigiendo que las agencias federales apliquen las correcciones antes del 10 de octubre de 2024.

Se aconseja encarecidamente a los usuarios que actualicen a la versión 5.0 de CSA lo antes posible, ya que la versión 4.6 ha alcanzado su fin de vida y ya no cuenta con soporte.