JumpCloud, un proveedor de soluciones de gestión de identidad y acceso en la nube, ha respondido rápidamente a un incidente de ciberseguridad en curso que ha afectado a algunos de sus clientes.

Como parte de sus esfuerzos para mitigar los daños, JumpCloud ha restablecido las claves de programación de aplicaciones (API) de todos los clientes afectados por este incidente, con el objetivo de proteger sus datos valiosos.

La empresa ha informado a los clientes afectados sobre la importancia crítica de esta acción, reafirmando su compromiso de salvaguardar sus operaciones y organizaciones. Sin embargo, este restablecimiento de claves de API implicará ciertas interrupciones en funcionalidades como la importación de AD, integraciones de HRIS, módulos de PowerShell de JumpCloud, aplicaciones de Slack de JumpCloud, aplicaciones sin servidor de Directory Insights, ADMU, paquetes MDM sin interacción de terceros, disparadores de comandos, integración de Okta SCIM, integración de Azure AD SCIM, Workato, Aquera, Tray, y más.

A pesar de las posibles molestias, JumpCloud sostiene que el restablecimiento de claves es en beneficio de sus clientes. Para aquellos que necesiten ayuda para restablecer o restablecer sus claves de API, la empresa está lista para brindar soporte.

La empresa insta a los clientes afectados a restablecer sus claves de API de manera rápida para mejorar la seguridad de sus sistemas. Para ayudar en este proceso, JumpCloud ha puesto a disposición una guía detallada y una simulación interactiva.

Este reciente suceso ha puesto de relieve la importancia de la seguridad de las API, evidenciando la necesidad de contar con medidas protectoras sólidas. Es fundamental que las empresas aseguren debidamente sus API para evitar posibles vulneraciones de seguridad.

Los servicios de Directorio Activo (AD) basados en la nube de JumpCloud son utilizados por

más de 180,000 organizaciones a nivel mundial. Numerosos proveedores de software y proveedores de servicios en la nube han integrado sus sistemas con la gama de servicios de gestión de identidad, acceso y dispositivos de JumpCloud.

No se disponen de detalles sobre la naturaleza específica o la magnitud del incidente en este momento, pero JumpCloud está abordando activamente la situación. Todavía no se ha determinado si la red de la empresa ha sido comprometida o cuál es la causa precisa del problema.

La forma en que JumpCloud ha comunicado la situación ha sido objeto de críticas por su falta de total transparencia.

Se recomienda a los clientes de JumpCloud afectados por este suceso que agilicen el restablecimiento de sus claves de API y estén atentos a futuros desarrollos o anuncios relacionados con este incidente.