El proveedor de servicios de identidad Okta reveló el viernes un nuevo incidente de seguridad en el que actores de amenazas no identificados lograron aprovechar credenciales robadas para acceder a su sistema de gestión de casos de soporte.

David Bradbury, director de seguridad de Okta, explicó que *«el actor de amenazas pudo visualizar archivos cargados por ciertos clientes de Okta como parte de casos de soporte recientes».* Es importante destacar que el sistema de gestión de casos de soporte de Okta es independiente del servicio principal de Okta, el cual se encuentra completamente operativo y no ha sido afectado.

La compañía subrayó que su sistema de gestión de casos Auth0/CIC no se vio comprometido por la brecha y se ha comunicado directamente con los clientes afectados.

Sin embargo, Okta señaló que el sistema de soporte al cliente se utiliza también para cargar archivos de Registro de Archivo HTTP (HAR) con el fin de replicar errores de usuarios finales o administradores para propósitos de solución de problemas.

Okta advirtió que los archivos HAR pueden contener datos sensibles, incluyendo cookies y tokens de sesión, que los actores malintencionados podrían utilizar para suplantar a usuarios legítimos.

La empresa también informó que trabajó con los clientes afectados para revocar los tokens de sesión incrustados y prevenir su uso indebido.

Okta no reveló la magnitud del ataque, la fecha exacta en que ocurrió el incidente ni cuándo se detectó el acceso no autorizado. Hasta marzo de 2023, Okta cuenta con más de 17,000 clientes y gestiona alrededor de 50 mil millones de usuarios.

En este contexto, se ha confirmado que BeyondTrust y Cloudflare son dos de los clientes que fueron blanco del último ataque al sistema de soporte.

> Cloudflare describió este ataque como sofisticado, ya que *«el actor de amenazas logró apoderarse de un token de sesión de un ticket de soporte creado por un empleado de Cloudflare. Utilizando el token obtenido de Okta, el actor de amenazas accedió a los sistemas de Cloudflare el 18 de octubre».*

Si bien Cloudflare resaltó que ningún cliente o sistema se vio afectado como resultado del evento, BeyondTrust señaló que notificó a Okta sobre la brecha el 2 de octubre de 2023. Sin embargo, el ataque a Cloudflare sugiere que el adversario mantuvo acceso a sus sistemas de soporte hasta al menos el 18 de octubre de 2023.

La empresa de servicios de gestión de identidad mencionó que su administrador de Okta había cargado un archivo HAR en el sistema el 2 de octubre para resolver un problema de soporte y que detectó actividad sospechosa relacionada con la cookie de sesión en un lapso de 30 minutos después de compartir el archivo. Los intentos de ataque contra BeyondTrust finalmente no tuvieron éxito.

> Un portavoz de BeyondTrust aseguró que *«la empresa detectó y solucionó de inmediato el ataque a través de sus propias herramientas de identidad, llamadas «Identity Security Insights», sin que esto tuviera ningún impacto o exposición en la infraestructura de BeyondTrust ni en sus clientes».*

Este incidente se suma a una serie de problemas de seguridad que han afectado a Okta en los últimos años. La empresa se ha convertido en un blanco de alto valor para grupos de hackers debido a que sus servicios de inicio de sesión único (SSO) son utilizados por algunas de las compañías más grandes del mundo.