Cyberattaque Okta : des mesures dÃ©fensives nÃ©cessaires
Internet
PostÃ© par : JerryG
PubliÃ©e le : 27/10/2023 13:00:00

L'entreprise amÃ©ricaine Okta a subi une cyberattaque et a indiquÃ© que Â« des attaquants ont rÃ©ussi Ã pÃ©nÃ©trer dans son systÃ¨me de support en utilisant des identifiants volÃ©s et en extrayant des jetons de session client valides Ã partir de fichiers de support tÃ©lÃ©chargÃ©s Â».

Tyler Reese, Director of Product Management chez Netwrix, a fait le commentaire suivant :

Â« Dans la mesure oÃ¹ cette attaque rÃ©cupÃ¨re les jetons sensibles qu'Okta avait en sa possession auprÃ¨s de son Ã©quipe d'assistance, la seule faÃ§on pour un client de se protÃ©ger est de prendre des mesures dÃ©fensives, car il n'existe aucune capacitÃ© raisonnable d'invalider de maniÃ¨re proactive ces jetons de la part du client.

Le premier ensemble de dÃ©fenses doit inclure une authentification matÃ©rielle forte pour les comptes privilÃ©giÃ©s et fonctionner Ã partir dâ□□un systÃ¨me fiable. Dans les cas documentÃ©s par BeyondTrust et Cloudflare, ils utilisaient des jetons matÃ©riels FIDO2 qui permettaient aux Ã©quipes de sÃ©curitÃ© d'exclure toute compromission potentielle des informations d'identification.

Le deuxiÃ¨me ensemble de dÃ©fenses devrait Ãªtre un audit robuste et une dÃ©tection des comptes privilÃ©giÃ©s Ã partir des systÃ¨mes dâ□□identitÃ©. Il a Ã©tÃ© mentionnÃ© dans l'un des rapports que mÃªme avec l'utilisation de FIDO2, le jeton compromis peut toujours Ãªtre utilisÃ© pour exÃ©cuter des appels API privilÃ©giÃ©s.

Le cybercriminel a tentÃ© de crÃ©er un compte privilÃ©giÃ© dÃ©guisÃ© en compte de service. GrÃ¢ce Ã une surveillance appropriÃ©e, cette activitÃ© a Ã©tÃ© dÃ©tectÃ©e Ã temps et le processus de crÃ©ation de comptes privilÃ©giÃ©s par porte dÃ©robÃ©e a Ã©tÃ© arrÃªtÃ©. Par la suite, ces comptes auraient pu Ãªtre utilisÃ©s une fois le jeton volÃ© expirÃ© et nâ□□Ã©taient plus exploitables.

En rÃ©sumÃ©, les clients auront besoin de dÃ©fenses d'authentification solides, ainsi que d'un audit et d'une dÃ©tection appropriÃ©s pour les modifications privilÃ©giÃ©es apportÃ©es Ã leur environnement Okta.

De maniÃ¨re gÃ©nÃ©rale, avec les attaques par supply chain, le plus grand dÃ©fi est l'imprÃ©visibilitÃ© : une fois qu'un fournisseur a Ã©tÃ© piratÃ©, il est difficile de savoir oÃ¹ le cybercriminel va se dÃ©placer avec ses privilÃ¨ges.

S'il s'agit d'un fournisseur de logiciels, il peut chercher Ã introduire des vulnÃ©rabilitÃ©s dans le logiciel. Sâ□□il sâ□□agit dâ□□un fournisseur de services financiers, il est susceptible de chercher Ã exfiltrer des donnÃ©es Ã des fins dâ□□extorsion. Le mieux que les organisations puissent faire est dâ□□adopter les concepts de lâ□□approche Zero Trust qui encouragent la surveillance, les moindres privilÃ¨ges, ainsi quâ□□une posture et une intÃ©gritÃ© solides des ressources IT dâ□□une organisation. Â»