TS PARTNERS
|630 Freedom Business Center Dr., Suite 212|
|King of Prussia, PA 19406|
|610.768.1100|

March 31, 2022

CVE-2021-34484 Breach of Okla by Lapsus$ Hacking Group

Question: "was TS Partners or products affected by Okta security breach by Lapsus$ extortion group?

Answer: NO –> read-on to understand more fully… **Action Required:** NONE

TS Partners does not itself use or require the Okta access management product in its applications. That said, a number of clients are known to use Okta at the enterprise-level of their organization. Clients may request that TS Partners leverage one of the enterprise services from Okta in the Client's use of TranStar.

In the context of TranStar, Okta can be used as the identity provider for single sign-on functionality – as an alternative to maintaining distinct operator logins. TranStar can integrate with the Client platform to use centralized domain-level SAML authentication.

Incident affecting Okta

On January 20, Okta Security team was alerted that a new factor (password) was added to the Okta account of a Sitel customer support engineer. Although that individual attempt was unsuccessful, Okta reset the account and notified Sitel, a third-party vendor that provides Okta customer support.

Sitel engaged a forensic firm to perform an investigation that confirmed an earlier attacker had access to a Sitel support engineer laptop for five-day period (Jan16-21, 2022). With fraudulent access, Lapsus$ obtained and shared screenshots online of Okta data obtained through the compromise of Sitel systems.

Okta has stated "As outlined in more detail in our blog, we have identified the customers that may have been impacted, and we have already contacted them. There is no impact to Auth0 or AtSpoke customers, and there is no impact to HIPAA and FedRAMP customers."

For Additional Information:
Okta Help Center – FAQs on January 2022 Compromise
https://support.okta.com/help/s/article/Frequently-Asked-Questions-Regarding-January-2022-Compromise?language=en_US

For questions regarding Policy, contact CEO or COO

Last Review: March 31, 2022
Last Revision: March 31, 2022