Sitel has been named as the third-party allegedly responsible for a recent security incident experienced by Okta.

In a [briefing](https://www.okta.com/blog/2022/03/oktas-investigation-of-the-january-2022-compromise/) on Wednesday, David Bradbury, Chief Security Officer at Okta, told virtual attendees that the incident has been "an embarrassment for myself and the entire Okta team."

Okta has become the subject of scrutiny following the leak of screenshots by the LAPSUS$ hacking group [earlier this week](https://www.zdnet.com/article/okta-says-breach-evidence-shared-by-lapsus-ransomware-group-linked-to-january-hack-attempt/). The images appeared to show that the attackers had [obtained access](https://www.zdnet.com/article/okta-revises-lapsus-impact-upwards-to-potentially-2-5-of-customers/) to "Okta.com Superuser/Admin and various other systems."

The identity and authentication services company said there was a five-day window in which the intrusion occurred.

"The report from the forensic firm highlighted that there was a five-day window of time between January 16 - 21, 2022, when the threat actor had access to the Sitel environment, which we validated with our own analysis," the CSO said.

According to Bradbury, a customer support engineer's laptop was the source of the intrusion, and the device was "owned and managed by Sitel."

Sitel is one of Okta's sub-processors. The executive said that the attackers used the remote desktop protocol (RDP) to access the laptop:

**"The scenario here is analogous to walking away from your computer at a coffee shop, whereby a stranger has (virtually in this case) sat down at your machine and is using the mouse and keyboard.**

**So while the attacker never gained access to the Okta service via account takeover, a machine that was logged into Okta was compromised and they were able to obtain screenshots and control the machine through the RDP session."**

After analyzing 125,000 login entries, the company now says that up to 366 customers may have been impacted.

An alert was issued on January 20 that a new multi-factor authentication (MFA) addition was "attempted" on the Sitel support engineer's account. The executive says that within "minutes", Okta sessions were terminated, pending an investigation. However, Bradbury claimed that the "attempted" MFA enrollment was "unsuccessful."

A day later, indicators of compromise (IoCs) were shared by Okta with Sitel, which also hired investigative help. Okta later received a summary of the incident, but the full report was not released until yesterday.

"I am greatly disappointed by the long period of time that transpired between our initial notification to Sitel in January and the issuance of the complete investigation report just hours ago," the CSO said. "Upon reflection, once we received the Sitel summary report last week, we should have, in fact, moved more swiftly to understand its implications."

Bradbury said that the 'Superuser' mode shown in the screenshots does not provide "god-like" access. Instead, support engineers can only use their accounts for "basic duties and handling inbound support queries."

As a result, the executive says that while the threat actor had access to the Sitel environment, it was "highly constrained."

"We are of the opinion that no corrective action needs to be taken by customers," Bradbury added.

However, in the interest of "transparency," potentially impacted customers will be sent an incident report.

"This incident will only serve to strengthen our commitment to security [...]," Bradbury commented. "We will continue to work tirelessly to ensure that you have a dependable and a secure, Okta service."