Okta said a hacker broke into its customer support ticket system and stole sensitive files

Description

Identity and access giant Okta said a hacker broke into its customer support ticket system and stole sensitive files that can be used to break into the networks of Okta's customers.

Okta chief security officer David Bradbury said in a blog post Friday that a hacker used a stolen credential to access the company's support case management system, which contained browser recording files uploaded by Okta customers for troubleshooting.

Browser recording sessions (or HAR files) are used for diagnosing problems during a web browsing session, and often include website cookies and session tokens, which if stolen can be used to impersonate a real user account without needing their password or two-factor.

Bradbury said "customers who were impacted by this have been notified." It's not clear how Okta's support case management system was initially compromised.

Okta provides organizations and companies with access and identity tools, such as "single sign-on," which allows employees access to all of a company's resources on the network with one set of credentials. Okta has around 17,000 customers and manages around 50 billion users, the company said in a March 2023 blog post.

Okta spokesperson Vitor De Souza told TechCrunch that around 1% of customers are affected by this breach, but declined to provide a specific number.

Security firm BeyondTrust, which uses Okta, said in its own blog post that it notified Okta of a potential breach on October 2 after it detected an attempted compromise to its network a short time after an administrator shared a browser recording session with an Okta support agent.

BeyondTrust's chief technology officer Marc Maiffret said the hacker used a session token from the uploaded browser recording session to create an administrator account on BeyondTrust's network, which it immediately shut down. Maiffret said the incident "was the result of Okta's support system being compromised which allowed an attacker to access sensitive files uploaded by their customers."

Security journalist Brian Krebs first reported the news. Krebs reported that Okta contained the incident by October 17, citing the company's deputy chief information security officer Charlotte Wylie.

This is the latest incident at Okta, which in 2022 said that hackers stole some of its source code. Earlier in 2022, hackers posted screenshots showing access to the company's internal network after hacking into a company Okta used for customer service.

Okta's stock closed down 11% on Friday following news of the breach.

Date
03/02/2025

Date Created

21/10/2023

Author

susantswain1