Okta System

//Okta says its support system was breached using stolen credentials

Okta says attackers accessed files containing cookies and session tokens uploaded by customers to its support management system after breaching it using stolen credentials.

"The threat actor was able to view files uploaded by certain Okta customers as part of recent support cases," said Okta's Chief Security Officer David Bradbury.

"It should be noted that the Okta support case management system is separate from the production Okta service, which is fully operational and has not been impacted."

Okta's CSO added that this incident did not impact the Autho/CIC case management system. Okta notified all customers' whose Okta environment

or support tickets were impacted by the incident. Those who haven't received an alert are not affected.

Session tokens and cookies likely exposed in the attack

While the company has yet to provide details on what customer information was exposed or accessed in the breach, the support case management system breached in this attack was also used to store HTTP Archive (HAR) files used to replicate user or administrator errors to troubleshoot various issues reported by users.

They also contain sensitive data, such as cookies and session tokens, which threat actors could use to hijack customer accounts.

"HAR files represent a recording of browser activity and possibly contain sensitive data, including the content of the pages visited, headers, cookies, and other data," Okta explains on its support portal.

"While this allows Okta staff to replicate browser activity and troubleshoot issues, malicious actors could use these files to impersonate you."

The company worked with affected customers during the incident investigation and revoked session tokens embedded in shared HAR files. It now advises all customers to sanitize their HAR files before sharing by ensuring they don't include credentials and cookies/session tokens.

Okta also shared a list of indicators of compromise observed during the investigation, including IP addresses and web browser User-Agent information linked to the attackers.

Multiple security incidents in less than 2 years

Last year, Okta disclosed that some of its customers' data was exposed after the Lapsus$ data extortion group gained access to its administrative consoles in January 2022.

One-time passwords (OTPs) delivered to Okta customers over SMS were also stolen by the Scatter Swine threat group (aka 0ktapus), which breached cloud communications company Twilio in August 2022.

Okta-owned authentication service provider Auth0 also disclosed in September that some older source code repositories were stolen from its environment using an unknown method.

Okta revealed its own source code theft incident in December after the company's private GitHub repositories were hacked.

An Okta spokesperson did not answer questions regarding the date of the breach and how many customers were affected when BleepingComputer reached out earlier today.

Instead, the spokesperson said the support system "is separate from the production Okta service, which is fully operational and has not been impacted. We have notified impacted customers and taken measures to protect all our customers."

Author - Himangshu Sarkar

Github - https://github.com/Himangshu30

LinkedIN - https://www.linkedin.com/in/himangshu-sarkar-b4ba3a22a