November 29, 2023

October Customer Support Security Incident - Update and Recommended Actions

David Bradbury

Related Posts: Root Cause Analysis [RCA] - Nov 3, 2023 / Security Incident - Oct 20, 2023

In the wake of the security incident Okta disclosed in October 2023 affecting our customer support management system (also known as the Okta Help Center), Okta Security has continued to review our initial analysis shared on November 3, re-examining the actions that the threat actor performed. This included manually recreating reports the threat actor ran in the system and the files the threat actor downloaded.

Today we are sharing new information that potentially impacts the security of our customers.

We have determined that the threat actor ran and downloaded a report that contained the names and email addresses of all Okta customer support system users. All Okta Workforce Identity Cloud (WIC) and Customer Identity Solution (CIS) customers are impacted except customers in our FedRamp High and DoD IL4 environments (these environments use a separate support system NOT accessed by the threat actor). The Auth0/CIC support case management system was also not impacted by this incident.

The threat actor ran a report on September 28, 2023 at 15:06 UTC that contained the following fields for each user in Okta's customer support system:

Created Date	Last Login	Full Name	Username	Email
Company Name	User Type	Address	[Date of] Last Password Change or Reset	Role: Name
Role: Description	Phone	Mobile	Time Zone	SAML Federation ID

The majority of the fields in the report are blank and the report does not include user credentials or sensitive personal data. For 99.6% of users in the report, the only contact information recorded is full name and email address.

While we do not have direct knowledge or evidence that this information is being actively exploited, there is a possibility that the threat actor may use this information to target Okta customers via phishing or social engineering attacks. Okta customers sign-in to Okta's customer support system with the same accounts they use in their own Okta org. Many users of the customer support system are Okta administrators. It is critical that these users have multi-factor authentication (MFA) enrolled to protect not only the customer support system, but also to secure access to their Okta admin console(s).

Given that names and email addresses were downloaded, we assess that there is an increased risk of phishing and social engineering attacks directed at these users. While 94% of Okta customers already require MFA for their administrators, we recommend ALL Okta customers employ MFA and consider the use of phishing resistant authenticators to further enhance their security. Please refer to product documentation to enable MFA for the admin console (Classic or OIE).

How we discovered this

Following the publication of the RCA on November 3, Okta Security reviewed our initial analysis of the actions that the threat actor performed, including manually recreating the reports that the threat actor ran within the customer support system. We identified that the file size of one particular report downloaded by the threat actor was larger than the file generated during our initial investigation. After additional analysis, we concluded that the report contained a list of all customer support system users. The discrepancy in our initial analysis stems from the threat actor running an unfiltered view of the report. Our November review identified that if the filters were removed from the templated report, the downloaded file was considerably larger - and more closely matched the size of the file download logged in our security telemetry.

We also identified additional reports and support cases that the threat actor accessed, which contain contact information of all Okta certified users and some Okta Customer Identity Cloud (CIC) customer contacts, and other information. Some Okta employee information was also included in these reports. This contact information does not include user credentials or sensitive personal data.

We are working with a third-party digital forensics firm to validate our findings and we will be sharing the report with customers upon completion.

Implementing recommended best practices

We recommend all customers immediately take the following actions to defend against potential attacks that target their Okta administrators.

- **Multi-Factor Authentication (MFA)**: We strongly recommend all Okta customers secure admin access using MFA at a minimum. We also strongly encourage customers to enroll administrative users in phishing resistant authenticators (such as Okta Verify FastPass, FIDO2 WebAuthn, or PIV/CAC Smart Cards) and to enforce phishing resistance for access to all administrative applications. Please refer to product documentation to enable MFA for the admin console (Classic or OIE).
- **Admin Session Binding**: As communicated in the Security Incident RCA, customers can now enable an Early Access feature in Okta that requires admins to reauthenticate if their session is reused from an IP address with a different ASN (Autonomous System Number). Okta strongly recommends customers enable this feature to further secure admin sessions.
- **Admin Session Timeout**: To align with NIST AAL3 guidelines and increase the security posture of every customer, Okta is introducing Admin Console timeouts that will be set to a default of 12-hour session duration and a 15-minute idle time. Customers will have the option to edit these settings. This will be available as an Early Access feature starting November 29th for preview orgs and December 4th for production orgs. The feature will be available for all production orgs by January 8th, 2024. An email was sent to all Super Admins regarding this change on November 27th, and a copy of that communication can be found in the Knowledge Base article: Admin Session Lifetime/Idle Timeout Security Enhancements.
- **Phishing Awareness**: In addition, Okta customers should be vigilant of phishing attempts that target their employees and especially wary of social engineering attempts that target their IT Help Desks and related service providers. We recommend Okta customers implement our industry-leading, phishing-resistant methods for enrollment, authentication, and recovery. Please see Okta Solutions for Phishing Resistance for more information on protecting your organization from phishing. We also strongly recommend that customers review their IT Help Desk verification processes and ensure that appropriate checks, such as visual verification, are performed before performing high risk actions such as password or factor resets on privileged accounts.

David Bradbury
Chief Security Officer

David Bradbury is Chief Security Officer at Okta. As CSO, he leads overall security execution for the organization and his team is responsible for navigating the evolving threat landscape to best protect employees and customers. In addition, he is instrumental in helping Okta's customers continue to adopt and accelerate Zero Trust security strategies.

Prior to joining Okta, Bradbury was Senior Vice President and Chief Security Officer at Symantec where he led and had global oversight of all cyber security and physical security programs.

Bradbury has built an international reputation for leading and delivering cybersecurity at scale. He has worked across his native Australia, as well as in the United Kingdom and the United States, leading highly-regarded security teams at some of the world's largest banks, including ABN AMRO, Barclays, Morgan Stanley and the Commonwealth Bank of Australia. He holds a B.S. in Computer Science from the University of Sydney.