August 31, 2023

Cross-Tenant Impersonation: Prevention and Detection

Defensive Cyber Operations

Summary

- Okta has observed attacks in which a threat actor used social engineering to attain a highly privileged role in an Okta customer Organization (tenant).
- When successful, the threat actor demonstrated novel methods of lateral movement and defense evasion.
- These methods are preventable and present several detection opportunities for defenders.

In recent weeks, multiple US-based Okta customers have reported a consistent pattern of social engineering attacks against their IT service desk personnel, in which the caller's strategy was to convince service desk personnel to reset all Multi-factor Authentication (MFA) factors enrolled by highly privileged users.

The attackers then leveraged their compromise of highly privileged Okta Super Administrator accounts to abuse legitimate identity federation features that enabled them to impersonate users within the compromised organization.

Tactics, Techniques and Procedures

Okta customers, the threat actor targeted users assigned with Super Administrator permissions.

- The threat actor would access the compromised account using anonymizing proxy services and an IP and device not previously associated with the user account.
- The compromised Super Administrator accounts were used to assign higher privileges to other accounts, and/or reset enrolled authenticators in existing administrator accounts. In some cases, the threat actor removed second factor requirements from authentication policies.
- The threat actor was observed configuring a second Identity Provider to act as an "impersonation app" to access applications within the compromised Org on behalf of other users. This second Identity Provider, also controlled by the attacker, would act as a “source” IdP in an inbound federation relationship (sometimes called “Org2Org”) with the target.
- From this “source” IdP, the threat actor manipulated the username parameter for targeted users in the second “source” Identity Provider to match a real user in the compromised “target” Identity Provider. This provided the ability to Single sign-on (SSO) into applications in the target IdP as the targeted user.

What is Inbound Federation?

Inbound Federation allows access to applications in a target Identity Provider (IdP) if the user has successfully authenticated to a source IdP. The feature can also be used for Just-in-time (JIT) provisioning of users. It’s a feature that is used to save months off mergers, acquisitions and divestitures. It is also popular with large organizations (such as global parent companies) that require central controls or globally provision one set of applications (while also empowering divisions to have some level of autonomy for their own policies and apps).

Given how powerful this is, access to create or modify an Identity Provider is limited to users with the highest permissions in an Okta organization - Super Administrator or Org Administrator. It can also be delegated to a Custom Admin Role to reduce the number of Super Administrator’s required in large, complex environments.

These recent attacks highlight why protecting access to highly privileged accounts is so essential.

leading, phishing-resistant methods for enrollment, authentication and recovery; restrict the use of highly privileged accounts, and apply dedicated access policies for administrative users and monitor and investigate anomalous use of functions reserved for privileged users.

A more detailed set of recommendations is listed below:

- Protect sign-in flows by enforcing phishing-resistant authentication with Okta FastPass and FIDO2 WebAuthn.
- Enable Protected Actions (under **Settings > Features**) to force re-authentication whenever an administrative user attempts to perform sensitive actions.
- Configure Authentication Policies (Application Sign-on Policies) for access to privileged applications, including the Admin Console, to require re-authentication “at every sign-in”.
- If using self-service recovery, initiate recovery with the strongest available authenticator, and limit recovery flows to trusted networks (by IP, ASN or geolocation).
- Review and consolidate the use of Remote Management and Monitoring (RMM) tools by help desk personnel, and block execution of all other RMM tools.
- Strengthen help desk identity verification processes using visual verification.
- Turn on and test New Device and Suspicious Activity end-user notifications.
- Take a "Zero Standing Privileges" approach to administrative access. Assign administrators Custom Admin Roles with the least permissions required for daily tasks, and require dual authorization for JIT (just-in-time) access to more privileged roles.
- Constrain custom help desk roles with resource sets that exclude groups of highly privileged administrators.
- Enforce dedicated admin policies - Assign all administrators to groups. Require users in these groups to sign-in from managed devices and via phishing resistant MFA (Okta FastPass, FIDO2 WebAuthn). Restrict this access to trusted Network Zones and deny access from anonymizing proxies.
- Apply ASN and IP Session Binding (from **Settings > Features**) to all administrative apps to prevent the replay of stolen administrative sessions.

TTPs listed above.

Stage of Attack	System Log Query	Workflows Templates/Further Advice
Detect AiTM phishing using FastPass	eventType eq "user.authentication.auth_via_mfa" AND result eq "FAILURE" AND outcome.reason eq "FastPass declined phishing attempt"	Monitor Unsuccessful Phishing Attempts
User Denied Access due to ASN/IP Session Binding	eventType eq "security.session.detect_client_roaming"	Support article
Alert on Factor Resets	eventType eq "user.mfa.factor.reset_all"	Trigger Notifications when All MFA Factors are Reset
Alert on Factor Downgrades	There is no System Log event for a Factor downgrade. To monitor all activation and deactivation events, use the following query: eventType sw "system.mfa.factor"	Tracking and Alerting for Possible Account Takeover Events
Alert on User Suspicious Activity Reports	eventType eq "user.account.report_suspicious_activity_by_enduser"	Suspicious Activity Reported
Alert on New Behaviors during Access to Okta Admin Console	eventType eq "policy.evaluate_sign_on" and target.displayName eq "Okta Admin Console" and debugContext.debugData.behaviors co "POSITIVE"	We recommend administrators use Expression Language to alert on access to the Admin Console from users that meet the following conditions:

	target.displayName eq "Okta Admin Console" and debugContext.debugData.LogOnlySecurityData co "POSITIVE"	
Alert on Sign-In Attempts via Anonymizing Proxies	eventType eq "user.session.start" and securityContext.isProxy eq "true"	We recommend administrators deny sign-ins from these services in policy using a Dynamic Network Zone.
Alert on Creation of an Identity Provider by a Super Administrator or Org Administrator	eventType eq "system.idp.lifecycle.create" Alternative that includes all creation and modification events: eventType sw "system.idp.lifecycle"	We recommend delegating access to this feature to a Custom Admin Role with the minimum required permissions.
Alert on Sign-In Events via a Third-Party Identity Provider	eventType eq "user.authentication.auth_via_IDP"	We recommend alerting on these events if the organization does not currently use the Inbound Federation feature.

Indicators of Compromise

For the period 2023-07-29 to 2023-08-19

IP addresses:

IP

98.113.77.43
108.21.89.22
75.252.4.33
73.205.234.246
99.25.84.9
185.56.83.225
96.244.225.43

Change Log

1.2 - Mar 8, 2024

- Updated recommendations to include new features released as part of Okta Secure Identity Commitment: Protected Actions, ASN/IP Session Binding.
- Updated detections section to include System Log event for for an authentication failure arising from session binding.

1.1 - Sep 9, 2023

- Updated Prevention section to include advice on constraining help desk administrators to specific user groups.
- Updated Detection section. While defenders can alert on IdP creation (eventType eq "system.idp.lifecycle.create"), an alternative approach is to alert on any creation or modification using the "starts with" qualifier (eventType sw "system.idp.lifecycle")

1.0 - Sep 1, 2023

- Original Version Published

The Defensive Cyber Operations (DCO) team is responsible for detecting and responding to cyber threats that impact Okta or our customers via the Okta platform. Our intelligence-driven capability identifies the adversaries most likely to impact Okta and our customers, and prioritises our defensive capabilities based on the threats most likely to be realised.