MITIGA

SNOWFLAKE CUSTOMERS
Find out fast if you are impacted by this active threat campaign. >>

BLOG

How Okta Passwords Can Be Compromised: Uncovering a Risk to User Data

By Doron Karmi Or Aspir

Abstract

Mitiga researchers have found a new potential post-exploitation attack method in Okta that enables adversaries to read users' passwords and credentials that are in the Okta audit logs. This knowledge can then allow adversaries to compromise Okta user accounts and access any resources or applications that they may have access to,

MITIGA

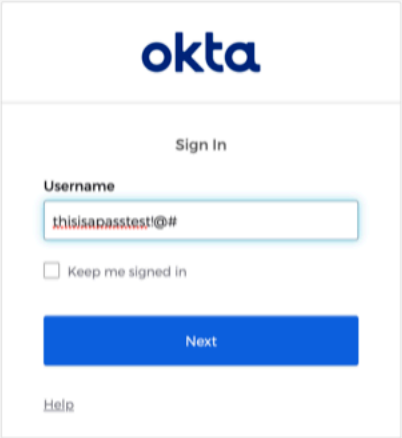
SNOWFLAKE CUSTOMERS
Find out fast if you are impacted by this active threat campaign. >>

passwords if they had been input incorrectly in the *username* field during login.

This exposure is possible because of the way Okta records failed login attempts to Okta instances. While it may seem like an edge case, this kind of password mistake is a common one for users. As a result, it poses a risk to many Okta customers.

What risk have we identified?

When a user logs in to their Okta domain, it's quite common for them to mistakenly enter their password in the *username* field on the login page, resulting in login failure. However, the unfortunate consequence of that action is that the failed login request is recorded in Okta audit logs, including the password in plain text in the *username* section. In most cases, users will subsequently do a successful login, registering the actual correct *username* in the log file.



As part of Mitiga's ongoing SaaS threat hunting activities, we analyzed the Okta audit logs for both successful and failed login attempts. We found that Okta's audit logs supply

MITIGA

SNOWFLAKE CUSTOMERS
Find out fast if you are impacted by this active threat campaign. >>

In our analysis, we discovered that passwords were present in the *username* field of failed login attempts. This is a concerning finding, as passwords should never be present in plain text in any type of log.

Feb 20 10:44:56	thisisatpasstest!@# (User)	User login to Okta failure: VERIFICATION_ERROR	Okta Dashboard (AppInstance)

Expand All

Actor	
AlternateId	thisisatpasstest!@#
DetailEntry	
DisplayName	unknown
ID	unknown
Type	User
Client	
Device	Computer
GeographicalContext	Tel AvivIsrael
ID	
IPAddress	188.120.157.187
UserAgent	CHROMEonMac OS X
Zone	null
Event	
AuthenticationContext	
DisplayMessage	User login to Okta
EventType	user.session.start
Outcome	
Published	2023-02-20T08:44:56.506Z
SecurityContext	
Severity	INFO
System	Transaction(id: Y_MzCFMfFvnQmZgix_TGGgAADnA)
Request	
IPChain	
Target	
AlternateId	Okta Dashboard
DetailEntry	
DisplayName	Okta Dashboard
ID	0oa47wuocv3v0KskL697
Type	AppInstance

MITIGA

SNOWFLAKE CUSTOMERS
Find out fast if you are impacted by this active threat campaign. >>

information could be used to escalate privileges in the case of exposed administrator' passwords.

To gain this user information, an attacker only needs the ability to read Okta audit logs. Here are a couple of examples of how an attacker would be able to read those logs.

User compromised

The audit logs are saved in the organization's SIEM solution such as Splunk. An attacker with permission to read the logs in the SIEM product, can harvest users' credentials. In addition, in such a scenario every user with read-only access to the SIEM solution (all SOC personnel) could potentially have access to other users' passwords, including Okta admins.

Supply-chain attacks

Third party services which have permissions to read Okta configuration. Products and services that integrate with Okta like CSPM products may request a "Read-only" Administrator role, which gives permissions to only read environment information. The role includes the ability to read the audit logs, which means those products/services could read users' credentials. So, in cases when those services/products get breached, the attacker can steal the Okta users' credentials.

How to know if your organization is affected?

To detect if user passwords have been mistakenly entered in the *username* field and are exposed in company logs, organizations can use their log analytics platform or SIEM where the Okta logs are stored. This type of security risk can occur in any organization that uses Okta for identity and access management. We have created a SQL query that can help companies identify these potential password exposures. However, this query

MITIGA

SNOWFLAKE CUSTOMERS
Find out fast if you are impacted by this active threat campaign. >>

```
, TO_DATE(published) as date_day
, date_part('HOUR', published) as date_hour
, get_json_object(debugContext, "$.debugData.deviceFingerprint") as deviceFingerprint
, src_ip
, src_useragent
, event_type
from
okta.okta_df
Where user_email <> 'system@okta.com'
)

, success as (
 SELECT
 user_email
, date_day
, date_hour
, deviceFingerprint
, src_ip
, src_useragent
FROM t0
WHERE event_type = 'core.user_auth.login_success'
)

, passw as (
SELECT
 user_email as password
, date_day
, date_hour
, deviceFingerprint
, src_ip
, src_useragent
FROM t0
WHERE event_type = 'core.user_auth.login_failed'
and length(user_email) >= 8
and user_email NOT LIKE '%@domain%'
and user_email NOT LIKE '%@domain%'
and user_email NOT LIKE '%.com'
and user_email NOT LIKE '0oa%'
and user_email RLIKE "(?=.*\d)(?=.*[a-z])(?=.*[A-Z])"

, joined as (
select
*
from success as s
JOIN passw as p using (date_day, date_hour, deviceFingerprint, src_ip, src_useragent)
ON p.date_day = s.date_day AND p.date_hour = s.date_hour AND p.src_ip = s.src_ip AND p.src_useragent = s.src_useragent AND p.deviceFingerprint = s.deviceFingerprint
)
```

Logic:

- Extract date and hour of the login attempt, device fingerprint, source IP address, and source user agent from raw Okta logs. (“t0” table)
- Filter for successful login attempts (event_type: core.user_auth.login_success) to create a "success" table.
- Filter for failed login attempts (event_type: core.user_auth.login_failed) with potential passwords in the user_email field to create a "passw" table.

MITIGA

SNOWFLAKE CUSTOMERS
Find out fast if you are impacted by this active threat campaign. >>

address, and source user agent to match *usernames* with their passwords.

Using this method, we were able to identify hundreds of potentially leaked passwords and credentials for our customers, including for administrator-level users.

Does multifactor authentication (MFA) alleviate this risk?

Multifactor authentication (MFA) is an effective way to enhance the security of user authentication in Okta. Okta admins can configure MFA at the organization or application level. With MFA, users are required to provide additional factors (such as a one-time password, biometric authentication, or a security token) in addition to their password when logging into Okta. This can help prevent unauthorized access even if attackers obtain users' credentials.

However, it's important to note that MFA is not foolproof, and attackers can still try to bypass it through various methods. For example:

- **Phishing**: Attackers can use social engineering techniques to trick users into providing their MFA credentials. This can include fake login pages or phishing emails that ask users to enter their MFA codes or accept the push notification from the authenticator app.
- **MFA fatigue**: Users can become overwhelmed with multiple MFA requests and begin to approve them without properly verifying the legitimacy of the request. Attackers can take advantage of this by sending a flood of MFA push notifications in a short time frame, causing the user to become fatigued and approve requests without thoroughly checking them. This allows the attacker to gain unauthorized access to the user's account.
- With access to the Okta logs, a threat actor could potentially wait for the perfect time to trigger MFA to circumvent it, by monitoring user's login pattern and

MITIGA

SNOWFLAKE CUSTOMERS
Find out fast if you are impacted by this active threat campaign. >>

In 2020, a series of phishing attacks targeted Okta customers, aiming to steal their MFA credentials. The attackers used various social engineering techniques to trick users into providing their credentials, including fake Okta login pages and phishing emails. Once the attackers obtained the MFA codes, they could bypass the MFA requirements and access the targeted accounts.

In another incident, a group of attackers used compromised credentials to access a victim's Okta account, which had MFA enabled. However, the attackers were able to bypass the MFA requirements by using a session hijacking technique. This allowed them to take over the victim's account and perform unauthorized activities.

Recommendations

To prevent potential post-exploitation attacks and unauthorized access to Okta, we recommend the following:

- **Use the SQL query**, which can be found on Mitiga's GitHub, to detect potential users that enter their password by mistake. Consider rotating their passwords.
- **Educate end-users**: Organizations should train their employees to avoid entering passwords in the *username* field on the Okta login page, as this can lead to credential theft.
- **Monitor audit logs**: Organizations should continuously monitor Okta audit logs for suspicious activities, including failed login attempts, and investigate any anomalies or security incidents promptly.
- **Implement MFA**: Organizations should enable MFA at the organization or application level to add an extra layer of security to user authentication. MFA can help prevent unauthorized access even if attackers obtain users' credentials.
- **Use SIEM securely**: If the organization is using a third-party SIEM solution to store audit logs, it is crucial to ensure that the solution is secure and properly

MITIGA

SNOWFLAKE CUSTOMERS
Find out fast if you are impacted by this active threat campaign. >>

Okta Response

"Okta has reviewed the reported issue and confirmed that it is expected behavior when users mistakenly enter their password in the username field. Okta logs failed login attempts and includes the erroneous username in the logs. These logs are only accessible to Okta administrators, who are the most privileged users in Okta and should be trusted not to engage in malicious activities."

We at Mitiga partially agree with Okta team. Typically, only users with at least "Read-only Administrator" role can read the logs in the Okta platform. However:

- Even if you are assigned with "Read-onlyAdministrator" role, it doesn't mean you should have ability to see users'passwords.
- Okta audit logs often get forwarded to a centralized security solution such as SIEM, which means other users that are not Okta administrators can read the logs.

Okta Recommendations

Okta recommends implementing the following strategies to avoid inadvertently logging passwords in the *username* field

- **Implement field validation**: Use client-side validation to check that the input in each field matches the expected format. Okta provides the ability to create custom character restrictions for the *username* field
- **Implement FastPass**: Okta FastPass is a feature that allows users to sign in with a single click or tap, without entering a *username* or password. FastPass uses biometric factors or device authentication to verify the user's identity, making it faster and more convenient for users to access their applications while maintaining a high level of security.

MITIGA

SNOWFLAKE CUSTOMERS
Find out fast if you are impacted by this active threat campaign. >>

(MFA) to further enhance the security of the Okta platform. By default, MFA is enforced when accessing the Okta Admin console. A bad actor would not be able to access the admin console without providing additional factors for login. Similarly, admins can set up an Authentication Policy that requires additional MFA when logging in to specific applications, which would further restrict what actions a bad actor can perform."

Summary

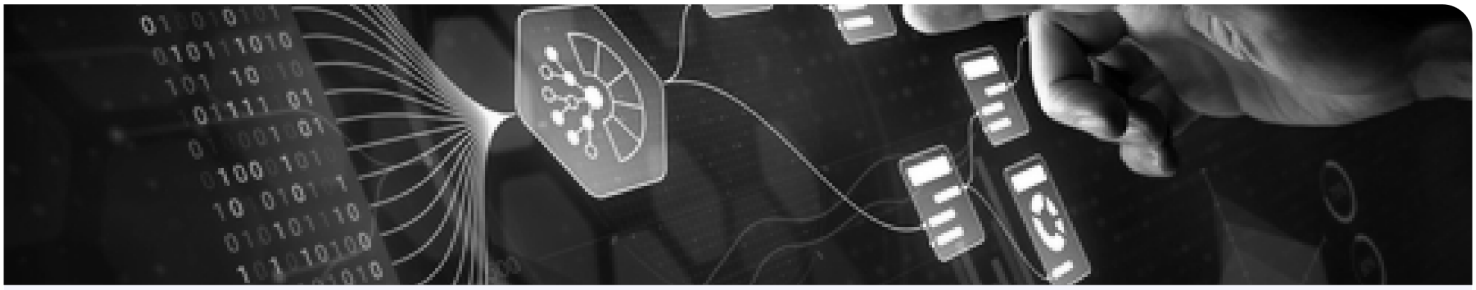
During our investigation, we discovered that some Okta logs inadvertently held passwords due to user error. This occurred when users accidentally entered their password in the *username* field. One of the ways attackers can fetch users' credentials is by reading the Okta audit logs from the SIEM product the organization uses. **Then the attackers can try to bypass the MFA through various methods**. Our team built a SQL query to match failed login attempts with a password pattern to subsequent successful login attempts, that you can use to detect if there are users' credentials in your Okta audit logs. We urge Okta users to be mindful of their login credentials and to ensure that passwords are entered correctly in the right field.

Don't miss these stories:

MITIGA

SNOWFLAKE CUSTOMERS
Find out fast if you are impacted by this active threat campaign. >>

prevention isn't enough..



Introducing Mitiga's Integration with Torq: Streamlining Cloud and SaaS Detection and Response Automation

Learn about the partnership between Mitiga and Torq that closes the gap in SecOps tools...

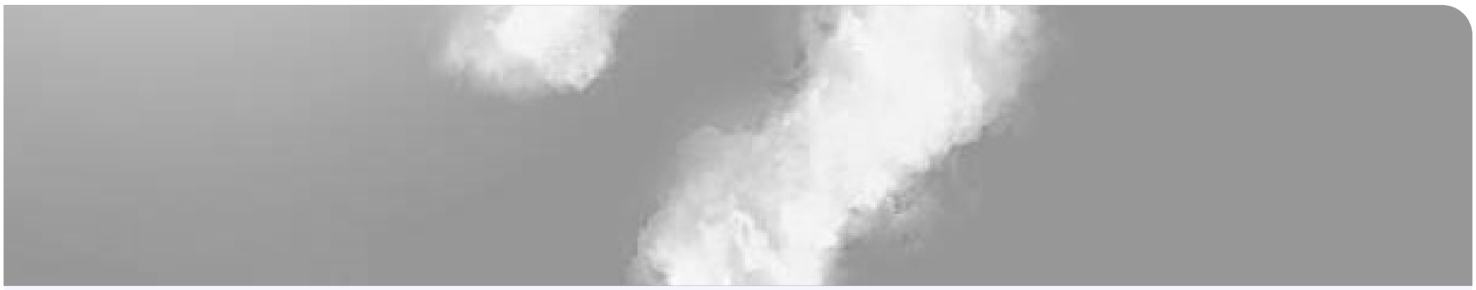
Why Cloud Threats in Healthcare are Surging and How to Combat Them

The healthcare industry is having an increasingly challenging time when it comes to cyber security..

MITIGA

SNOWFLAKE CUSTOMERS
Find out fast if you are impacted by this active threat campaign. >>

Microsoft experienced an issue with internal monitoring agents, resulting in incomplete logs for some services..



What the Wiz Acquisition of Gem Security Means for the Future of Cloud Threat Detection, Investigation, and Response

It's official: Gem Security is joining CNAPP decacorn Wiz.

6 Keys to Resiliency in the Cloud: Advice for CISOs

Enterprise success relies on operational resilience.

MITIGA

SNOWFLAKE CUSTOMERS
Find out fast if you are impacted by this active threat campaign. >>

The best response to your next breach starts now

SOLUTIONS **CAREERS**
BLOG **CONTACT**
ABOUT

Copyright © Mitiga Security Inc. All rights reserved | Terms of Use | Privacy Policy