THREAT ADVISORY

May 30, 2024

Okta CIC Credential Stuffing

SUMMARY

Okta issued a warning regarding a vulnerability in the cross-origin authentication feature of its Customer Identity Cloud (CIC) that is susceptible to credential stuffing attacks; stating:

> *"Okta researchers have detected that the endpoints supporting this cross-origin authentication feature are being targeted by credential stuffing attacks affecting several of our customers."*

TECHNICAL DETAILS

Suspicious activity began on April 15, 2024, with Okta proactively notifying customers who had the cross-origin authentication feature enabled. Okta did not disclose how many customers were affected by the attacks.

Credential stuffing is a cyberattack where threat actors use lists of usernames and passwords obtained from previous data breaches, phishing, or malware campaigns to attempt logins to online services.

This attack vector comes just a month after Okta reported a rise in the frequency and scale of credential stuffing attacks on online services, facilitated by the use of residential proxy services.

RECOMMENDATIONS

- Review Tenant Logs for unexpected login events, including failed cross-origin authentication (fcoa), successful cross-origin authentication (scoa), and breached password (pwd_leak) events.
- Rotate Credentials Regularly, changing passwords and credentials to reduce the risk of unauthorized access.
- Restrict or Disable Cross-Origin Authentication by limiting or turning off the cross-origin authentication feature for tenants.
- Enable Breached Password Detection by Activating breached password detection or use Credential Guard to identify and prevent the use of compromised passwords.
- Prohibit Weak Passwords by Enforcing policies that prevent users from choosing weak or easily guessable passwords.
- Adopt Passwordless Authentication by Enrolling users in passwordless, phishing-resistant authentication methods using new standards like passkeys.

REFERENCES

- https://sec.okta.com/articles/2024/05/detecting-cross-origin-authentication-credential-stuffing-attacks
- https://thehackernews.com/2024/05/okta-warns-of-credential-stuffing.html