How Cloudflare mitigated yet another Okta compromise

2023-10-20

 Sourov Zaman

 Lucas Ferreira

 Kimberly Hall

 Grant Bourzikas

3 min read

This post is also available in 简体中文, 日本語, 한국어 and 繁體中文.

On Wednesday, October 18, 2023, we discovered attacks on our system that we were able to trace back to Okta – threat actors were able to leverage an authentication token compromised at Okta to pivot into Cloudflare's Okta instance. While this was a troubling security incident, our Security Incident Response Team's (SIRT) real-time detection and prompt response enabled containment and minimized the impact to Cloudflare systems and data. We have verified that **no Cloudflare customer information or systems were impacted by this event** because of our rapid response. Okta has now released a public statement about this incident.

This is the second time Cloudflare has been impacted by a breach of Okta's systems. In March 2022, we blogged about our investigation on how a breach of Okta affected Cloudflare. In that incident, we concluded that there was no access from the threat actor to any of our systems or data – Cloudflare's use of hard keys for multi-factor authentication stopped this attack.

The key to mitigating this week's incident was our team's early detection and immediate response. In fact, we contacted Okta about the breach of their systems before they had notified us. The attacker used an open session from Okta, with Administrative privileges, and accessed our Okta instance. We were able to use our Cloudflare Zero Trust Access, Gateway, and Data Loss Prevention and our Cloudforce One threat research to validate the scope of the incident and contain it before the attacker could gain access to customer data, customer systems, or our production network. With this confidence, we were able to quickly mitigate the incident before the threat-actors were able to establish persistence.

According to Okta's statement, the threat-actor accessed Okta's customer support system and viewed files uploaded by certain Okta customers as part of recent support cases. It appears that in our case, the threat-actor was able to hijack a

session token from a support ticket which was created by a Cloudflare employee. Using the token extracted from Okta, the threat-actor accessed Cloudflare systems on October 18. In this sophisticated attack, we observed that threat-actors compromised two separate Cloudflare employee accounts within the Okta platform. We detected this activity internally more than 24 hours before we were notified of the breach by Okta. Upon detection, our SIRT was able to engage quickly to identify the complete scope of compromise and contain the security incident. Cloudflare's Zero Trust architecture protects our production environment, which helped prevent any impact to our customers.

Recommendations for Okta

We urge Okta to consider implementing the following best practices, including:

- Take any report of compromise seriously and act immediately to limit damage; in this case Okta was first notified on October 2, 2023 by BeyondTrust but the attacker still had access to their support systems at least until October 18, 2023.
- Provide timely, responsible disclosures to your customers when you identify that a breach of your systems has affected them.
- Require hardware keys to protect all systems, including third-party support providers.

For a critical security service provider like Okta, we believe following these best practices is table stakes.

Recommendations for Okta's Customers

If you are an Okta customer, we recommend that you reach out to them for further information regarding potential impact to your organization. We also advise the following actions:

- Enable Hardware MFA for all user accounts. Passwords alone do not offer the necessary level of protection against attacks. We strongly recommend the usage of hardware keys, as other methods of MFA can be vulnerable to phishing attacks.
- Investigate and respond to:
    - All unexpected password and MFA changes for your Okta instances.
    - Suspicious support-initiated events.
    - Ensure all password resets are valid and force a password reset for any under suspicion.
    - Any suspicious MFA-related events, ensuring only valid MFA keys are present in the user's account configuration.
- Monitor for:
    - New Okta users created.
    - Reactivation of Okta users.
    - All sessions have proper authentication associated with it.
    - All Okta account and permission changes.
    - MFA policy overrides, MFA changes, and MFA removal.

    - Delegation of sensitive applications.
    - Supply chain providers accessing your tenants.
- Review session expiration policies to limit session hijack attacks.
- Utilize tools to validate devices connected to your critical systems, such as Cloudflare Access Device Posture Check.
- Practice defense in depth for your detection and monitoring strategies.

Cloudflare's Security and IT teams continue to remain vigilant after this compromise. If further information is disclosed by Okta or discovered through additional log analysis, we will publish an update to this post.

Cloudflare's Security Incident Response Team is hiring.

Cloudflare's connectivity cloud protects entire corporate networks, helps customers build Internet-scale applications efficiently, accelerates any website or Internet application, wards off DDoS attacks, keeps hackers at bay, and can help you on your journey to Zero Trust.

Visit 1.1.1.1 from any device to get started with our free app that makes your Internet faster and safer.

To learn more about our mission to help build a better Internet, start here. If you're looking for a new career direction, check out our open positions.

Y Discuss on Hacker News

Okta | Post Mortem | 1.1.1.1

Follow on X

Lucas Ferreira | @lucassapao
Grant Bourzikas | @GrantBourzikas
Cloudflare | @cloudflare

RELATED POSTS

October 15, 2024 3:00 PM

Protect against identity-based attacks by sharing Cloudflare user risk scores with Okta

Uphold Zero Trust principles and protect against identity-based attacks by sharing Cloudflare user risk scores with Okta. Learn how this new integration allows your organization to mitigate risk in real time, make informed access decisions, and free up security resources with automation....

By Noelle Kagan, Andrew Meyer, James Chang, Gavin Chen, Matt Davis

Cloudflare Zero Trust, Okta, Partners

September 24, 2024 3:00 PM

Cloudflare partners with Internet Service Providers and network equipment providers to deliver a safer browsing experience to millions of homes

Cloudflare is extending the use of our public DNS resolver through partnering with ISPs and network providers to deliver a safer browsing experience directly to families. Join us in protecting every Internet user from unsafe content with the click of a button, powered by 1.1.1.1 for Families....

By Kelly May Johnston, Morgan Steffen

Birthday Week, 1.1.1.1, Privacy, DNS, Security, Partners, Network Services

July 04, 2024 3:00 PM

Cloudflare 1.1.1.1 incident on June 27, 2024

On June 27, 2024, a small number of users globally may have noticed that 1.1.1.1 was unreachable or degraded. The root cause was a mix of BGP (Border Gateway Protocol) hijacking and a route leak...

By Bryton Herdes, Mingwei Zhang, Tanner Ryan

1.1.1.1, Outage

June 26, 2024 3:00 PM

Cloudflare incident on June 20, 2024

A new DDoS rule resulted in an increase in error responses and latency for Cloudflare customers. Here's how it went wrong, and what we've learned...

By Lloyd Wallis, Julien Desgats, Manish Arora

Post Mortem, Outage