


DATA
CONOMY

NEWSAIBIG DATAMACHINE LEARNINGTRENDS ▾INDUSTRY ▾EVENTSJOBABOUT ▾

f

in

SUBSCRIBE



Breaking down the Okta Data Breach: What happened?

The Okta data breach, a recent incident, exposed vulnerabilities in digital identity security, underscoring the critical need for robust safeguards in an interconnected world.

by Eray Eliçık — October 23, 2023 in Cybersecurity

Home > Cybersecurity



Utilisation de Cookies et de Données Personnelles

Sur ce site Internet, nous utilisons des cookies et des fonctions similaires pour traiter les informations sur les terminaux et les données personnelles (par exemple, les adresses IP ou les informations du navigateur). Le traitement est utilisé à des fins telles que l'intégration de contenus, de services externes et d'éléments de tiers, l'analyse/mesure statistique, la publicité personnalisée et l'intégration des médias sociaux. Selon la fonction, les données sont transmises à [132 tiers](#) et traitées par eux. Ce consentement est volontaire, n'est pas nécessaire à l'utilisation de notre site Internet et peut être révoqué à tout moment à l'aide de l'icône en bas à gauche.

Stocker et/ou accéder à des informations sur un appareil

Utiliser des données limitées pour sélectionner la publicité

Créer des profils pour la publicité personnalisée

Utiliser des profils pour sélectionner des publicités personnalisées

Refuser tout

Paramètres

Tout accepter

efforts to protect your digital identity. Strap in, for we're about to embark on a journey through the intricate world of cyber threats and resilience.

LATEST ARTICLES

Can you ever guarantee income or growth from investments?

Navigating the evolving landscape of fiat money and cryptocurrencies

Does ChatGPT Search mean the end for traditional search engines?

Stable Diffusion 3.5 Medium is launched for consumer-level GPUs

Tech industry became plagued with ghost jobs

Android 15 QPR2 Beta 2 release date unveiled

Okta data breach unveiled

The Okta data breach is an incident that occurred when a threat actor gained unauthorized access to certain parts of Okta's infrastructure, potentially compromising sensitive data. Okta is a well-known company specializing in identity and

This website uses cookies. By continuing to use this website you are giving consent to cookies being used. Visit our [Privacy Policy](#). I Agree

Page 1 of 4

and businesses. This breach raised significant concerns due to the potential impact on the security and privacy of customer data.



The Okta data breach, a significant cybersecurity incident in October 2023, highlighted the importance of strengthening digital identity security measures and safeguarding sensitive user data in today's interconnected digital landscape ([Image credit](#))

Utilisation de Cookies et de Données Personnelles

Sur ce site Internet, nous utilisons des cookies et des fonctions similaires pour traiter les informations sur les terminaux et les données personnelles (par exemple, les adresses IP ou les informations du navigateur). Le traitement est utilisé à des fins telles que l'intégration de contenus, de services externes et d'éléments de tiers, l'analyse/mesure statistique, la publicité personnalisée et l'intégration des médias sociaux. Selon la fonction, les données sont transmises à [132 tiers](#) et traitées par eux. Ce consentement est volontaire, n'est pas nécessaire à l'utilisation de notre site Internet et peut être révoqué à tout moment à l'aide de l'icône en bas à gauche.

Stocker et/ou accéder à des informations sur un appareil

Utiliser des données limitées pour sélectionner la publicité

Créer des profils pour la publicité personnalisée

Utiliser des profils pour sélectionner des publicités personnalisées

Refuser tout

Paramètres

Tout accepter

alerted Okta

- October 3, 2023 – Asked Okta support to escalate to Okta security team given initial forensics pointing to a compromise within Okta support organization
- October 11, 2023 and October 13, 2023 – Held Zoom sessions with Okta security team to explain why we believed they might be compromised
- October 19, 2023 – Okta security leadership confirmed they had an internal breach, and BeyondTrust was one of their affected customers.
- **Delay in confirmation:** BeyondTrust promptly informed Okta of their findings on the same day, but it took Okta more than two weeks to confirm the breach. During this time, BeyondTrust continued to escalate the issue within Okta.
- **Support case management system compromised:** The threat actor gained access to Okta’s support case management system, which is separate from the main Okta service. This system is used for managing customer support tickets and related data.
- **Sensitive data exposed:** While specific details about the exposed data were not disclosed, it is known that the breached system contained HTTP Archive (HAR) files. These files are used to record browser activity for troubleshooting purposes. They include sensitive data like cookies and session tokens, which are

potentially misuse this information to impersonate users or hijack their accounts.

- **Cloudflare involvement:** Cloudflare, another prominent web infrastructure and security company, also detected malicious activity linked to the Okta breach on its servers. The attackers used an authentication token stolen from Okta's support system to gain access to Cloudflare's Okta instance, which had administrative privileges. However, Cloudflare's security team acted swiftly to contain the threat, ensuring that no customer information or systems were impacted.
- **Impact on customers:** Okta has taken measures to notify customers whose environments or support tickets were impacted by the breach. If customers have not received an alert, their data remains secure. Okta has also advised customers to sanitize their HAR files before sharing them to prevent the exposure of sensitive credentials and tokens.
- **Indicators of compromise:** Okta shared a list of indicators of compromise observed during their investigation, including IP addresses and web browser User-Agent information linked to the attackers. This information can help organizations identify and respond to potential security threats.
- **Previous incidents:** It's worth noting that Okta had experienced security incidents in the past. In January 2022, some customer data was exposed when the Lapsus\$ data extortion group gained access to Okta's administrative consoles. In August 2022, one-time passwords (OTPs) delivered to Okta customers over SMS

Utilisation de Cookies et de Données Personnelles

Sur ce site Internet, nous utilisons des cookies et des fonctions similaires pour traiter les informations sur les terminaux et les données personnelles (par exemple, les adresses IP ou les informations du navigateur). Le traitement est utilisé à des fins telles que l'intégration de contenus, de services externes et d'éléments de tiers, l'analyse/mesure statistique, la publicité personnalisée et l'intégration des médias sociaux. Selon la fonction, les données sont transmises à [132 tiers](#) et traitées par eux. Ce consentement est volontaire, n'est pas nécessaire à l'utilisation de notre site Internet et peut être révoqué à tout moment à l'aide de l'icône en bas à gauche.

🍪 Stocker et/ou accéder à des informations sur un appareil

📄 Utiliser des données limitées pour sélectionner la publicité

👤 Créer des profils pour la publicité personnalisée

🔗 Utiliser des profils pour sélectionner des publicités personnalisées

Refuser tout

Paramètres

Tout accepter









This breach highlights the ongoing challenges and threats in the world of cybersecurity, emphasizing the need for robust security practices and measures. Okta and its partners have been actively working to address the situation and enhance their security to prevent such incidents in the future. The incident serves as a reminder of the importance of vigilance and prompt response in safeguarding sensitive data.

For more detailed information, click [here](#).

Tags: [Data Breach](#) [hack](#) [leak](#) [okta](#)

Related Posts

	Cash app data breach compensation: How to get what you're owed 🕒 OCTOBER 30, 2024		Change Healthcare data breach: What to do 🕒 OCTOBER 25, 2024
	Internet Archive is breached again 🕒 OCTOBER 21, 2024		ChatGPT-4o is hacked: It is giving away drug recipes 🕒 OCTOBER 16, 2024
	Cisco data breach: Hackers accessed to source code 🕒 OCTOBER 15, 2024		Central Tickets data breach: Everything you need to know 🕒 OCTOBER 14, 2024



Utilisation de Cookies et de Données Personnelles

Sur ce site Internet, nous utilisons des cookies et des fonctions similaires pour traiter les informations sur les terminaux et les données personnelles (par exemple, les adresses IP ou les informations du navigateur). Le traitement est utilisé à des fins telles que l'intégration de contenus, de services externes et d'éléments de tiers, l'analyse/mesure statistique, la publicité personnalisée et l'intégration des médias sociaux. Selon la fonction, les données sont transmises à [132 tiers](#) et traitées par eux. Ce consentement est volontaire, n'est pas nécessaire à l'utilisation de notre site Internet et peut être révoqué à tout moment à l'aide de l'icône en bas à gauche.

- 🕒 Stocker et/ou accéder à des informations sur un appareil
- 🔑 Utiliser des données limitées pour sélectionner la publicité
- 🕒 Créer des profils pour la publicité personnalisée
- 🔑 Utiliser des profils pour sélectionner des publicités personnalisées

Refuser tout

Paramètres

Tout accepter

