Case Study

Session Hijacking

Okta data breach

Attack Category:
Session Hijacking

Okta Data Breach

1. On October 2023 a data breach affect customer support system users.

2. Less than 1% of the company’s customers that could be used to hijack Okta sessions of legitimate users .

Sources for your research:

Bleeping Computer
URL: Bleepingcomputer.com.

By Bill Toulas.

Company Description and Breach Summary

Okta is an American identity and access management company based in San Francisco.It provides cloud software That’s helps companies manage and secure user authentication into applications.

According to details uncovered at the time, the hacker accessed HAR files with cookies and session tokens for 134 customers.

Timeline

1. Event 1
Otka’s invertigated a breach from its help center environment revealed that the hackers obtained data belonging to all customers support system users.

2. Event 2
The company note that the threat actor also accessed additional reports cases with contact information.

3. Event 3
At the beginning of November, the company disclosed that the threat actor had gained unauthorized access to file inside customers support system.

4. Event 4
The hacker accessed HAR files with cookies and session tokens for 134 customers.

5. Event 5
The threat actor also Downloaded a report that contain the names and Email addresses of all Okta customers.

6. Event 6: According to the company the stolen report included fields like fullname, username, email, company name, address, last password change, role phone number.

Vulnerabilities

By session hijacking unauthorized access was granted to the threat actor, the result is a data breach of the personal informations downloaded by the threat actor.

Vulnerability 1

Cross-Site Scripting XSS

Vulnerability 2

Social Engineering.

Vulnerability 3

Identification and Authentification Failures.

Vulnerability 4

Phishing Attack

Costs and Prevention

Costs

- Ultimately wiping out $ 2 billions in market cap and Okta’s share plummeted by 11 %.

Prevention

- Implement MFA for admin access.
- Using phishing-resistant like FastPass, Fido2 WebAuthn, Smart Cards.
- Set admin session timeouts to 15 minutes as per NIST guidelines.
- Increase phishing awareness by staying vigilant.