مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

United Arab Emirates

Exploited Vulnerability-Okta Classic Application

Tracking #:432316371

Date:08-10-2024

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed Okta has recently resolved a vulnerability that could have allowed attackers to bypass sign-on policies and gain unauthorized access to applications.

TECHNICAL DETAILS:

Vulnerability Overview:

- **Date Identified**: September 27, 2024
- **Affected Product**: Okta Classic (as of July 17, 2024)
- **Resolution Date**: October 4, 2024
- **Nature of Vulnerability**: The vulnerability enabled an attacker with valid credentials to bypass application-specific sign-on policies, which could include network zones, device-type restrictions, or other authentication requirements.

Exploitation Conditions:

For exploitation to occur, the following conditions had to be met:

1. Possession of a valid username and password.
2. Organization configured with application-specific sign-on policies.
3. Use of a user-agent classified by Okta as “unknown” (e.g., uncommon browsers or scripts).

RECOMMENDATIONS:

Organizations using Okta Classic should take the following steps:

1. **Log Review**:
   - Review the Okta System Log for unexpected authentications from user-agents classified as “unknown” between July 17 and October 4.
2. **Activity Monitoring**:
   - Search for any prior activity before July 17, 2024. If a user authenticated with the same "unknown" user-agent previously, it may indicate legitimacy.
   - Look for unsuccessful authentication attempts leading up to successful logins, which could suggest credential-based attacks.
   - Monitor for deviations in user behavior such as unusual geolocations or IP addresses.
3. **Policy Review**:
   - Pay special attention to applications with default policy rules that cannot be configured by customers (e.g., Microsoft Office 365 and Radius).

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- https://trust.okta.com/security-advisories/okta-classic-application-sign-on-policy-bypass-2024