مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Security Updates- Okta

Tracking #:432316465

Date:04-11-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that Okta has released security updates to address a high-severity vulnerability in Okta Verify Desktop MFA for Windows.

TECHNICAL DETAILS:

Okta has released security updates addressing a high-severity vulnerability in its Okta Verify Desktop MFA for Windows. The flaw, identified as CVE-2024-9191, could potentially allow attackers to steal user passwords associated with the passwordless login feature within Okta Device Access.

Vulnerability Details:

- **CVE ID**: CVE-2024-9191
- **CVSS Score**: 7.1 (High)
- **Impacted Component**: OktaDeviceAccessPipe
- The vulnerability allows attackers with access to a compromised device to retrieve passwords associated with Desktop MFA passwordless logins through the OktaDeviceAccessPipe. This could lead to unauthorized access to user accounts and connected applications.

Affected Versions:

- Okta Verify for Windows versions 5.0.2 to 5.3.2

Fixed Versions:

- Okta Verify for Windows to version 5.3.3 or later

RECOMMENDATIONS:

The UAE Cyber Security Council recommends to upgrade the affected versions to the fixed versions at the earliest.

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-verify-desktop-mfa-for-windows-passwordless-login-cve-2024-9191/