M1: Improper Credential Usage

Deskripsi

Kerentanan terjadi ketika aplikasi gagal mengelola kredensial pengguna, misalnya dengan menyimpannya pada source code aplikasi, atau menyimpan kredensial pada tempat yang tidak aman. Threat agent dapat mendeteksi lokasi penyimpanan kredensial untuk eksploitasi lebih lanjut.

Kerentanan disebabkan antara lain:

- **Hardcoded Credentials** - Aplikasi menyimpan kredensial pengguna di dalam source code atau file konfigurasi.
- **Insecure Credential Transmission** - Kredensial dikirimkan tanpa enkripsi atau melalui saluran yang tidak aman.
- **Insecure Credential Storage** - Aplikasi menyimpan krendensial pengguna pada perangkat yang tidak diamankan.
- **Weak User Authentication** -Otentikasi pengguna menggunakan protokol yang lemah atau mudah dilewati.

Dampak

- teknis - Pengelolaan kredensial yang buruk dapat mengakibatkan dampak teknis yang signifikan. Pihak yang tidak sah dapat mengakses informasi sensitif atau fungsi aplikasi atau sistem backend sehingga menyebabkan kebocoran data, kehilangan privasi, tindakan fraud, atau akses administratif.
- Bisnis - Berdampak signifikan antara lain menurunnya reputatasi, pencurian informasi, fraud dan akses tidak sah terhadap data.

Mitigasi

- Tidak menyimpan kredensial pengguna dalam source aplikasi atau file konfigurasi tertentu pada aplikasi/
- Tidak menyimpan kredensial pengguna pada perangkat.
- Menerapkan protokol otentikasi pengguna yang kua.
- Memperbarui dan mengganti API key atau token secara berkala.

Revision #2
Created 2 October 2024 07:01:38 by Tim Persandian
Updated 2 October 2024 07:35:25 by Tim Persandian