

A08:2021 - Software and Data Integrity Failures

Deskripsi

Software and Data Integrity Failures merupakan kondisi keaslian, konsistensi, dan keamanan perangkat lunak serta data tidak dapat dipastikan. Kegagalan integritas ini dapat disebabkan oleh berbagai faktor diantaranya:

- Kerentanan dalam source code, serangan siber, dan penggunaan komponen perangkat lunak yang tidak aman
- Kode dan infrastruktur yang tidak mencegah terjadinya pelanggaran integritas
- Aplikasi yang bergantung pada *plugins*, *libraries*, atau *modules* dari sumber yang tidak dipercaya dan *pipeline* yang tidak aman.
- Pembaharuan otomatis yang diunduh tanpa adanya verifikasi integritas.

Dampak

Akses ilegal/tidak sah, kode yang berbahaya, atau kerusakan sistem.

Mitigasi

- Menggunakan tanda tangan digital atau mekanisme yang sama untuk memverifikasi bahwa perangkat lunak atau data berasal dari sumber yang diharapkan dan tidak dimanipulasi.
- Memastikan *libraries* dan dependensi seperti npm atau maven menggunakan repositori yang terpercaya.
- Memastikan keamanan rantai pasokan perangkat lunak dengan memverifikasi bahwa komponen tersebut tidak memiliki kerentanan yang sudah diketahui.
- Memastikan adanya proses review ketika mengubah kode dan konfigurasi untuk meminimalisir kemungkinan kode atau konfigurasi berbahaya masuk ke dalam *pipeline* perangkat lunak anda.
- Memastikan *CI/CD pipeline* anda memiliki metode pemisahan, konfigurasi dan akses kontrol yang tepat untuk memastikan integritas kode yang masuk mulai dari proses *build* / pembangunan hingga proses *deployment* / penyebaran perangkat lunak.

- Memastikan data yang belum di tandatangani atau tidak terenkripsi ini tidak terkirim ke klien yang tidak dipercaya tanpa adanya pengecekan integritas atau tanda tangan digital untuk mendeteksi apakah data telah di manipulasi atau pemutaran ulang data yang telah di serialisasi.

Revision #1

Created 4 September 2024 04:09:01 by Tim Persandian

Updated 4 September 2024 04:20:51 by Tim Persandian