A05:2021 - Security Misconfiguration

Deskripsi

Security misconfiguration merupakan kondisi sistem komputer, aplikasi, atau infrastruktur IT tidak dikonfigurasi dengan baik untuk melindungi informasi sensitif dan sumber daya organisasi dari ancaman keamanan. Konfigurasi yang salah atau kurangnya pembaruan pada sistem dan aplikasi dapat menciptakan celah keamanan yang dapat dimanfaatkan oleh penyerang. Hal ini sering disebabkan oleh:

- Kelalaian dalam pengelolaan konfigurasi keamanan atau kurangnya pemahaman mengenai praktik keamanan yang terbaik.
- Tidak memiliki pertahanan yang sesuai atau *security hardening* yang diperlukan
- Fitur - fitur yang tidak digunakan masih di enable atau diinstall
- Menggunakan akun dan password default atau tidak pernah diubah.
- Cara menghandle error terlalu informatif kepada user
- Tidak menggunakan fitur keamanan terbaru.
- Pengaturan security pada server aplikasi, framework aplikasi tidak diatur secara aman.
- Server tidak mengirim *security header* atau directives, atau tidak diatur secara aman..
- Menggunakan software yang tidak *update* atau rentan.

Dampak

Ekploitasi terhadap celah konfigurasi.

Mitigasi

- Melakukan otomasi terhadap proses *hardening* untuk meminimalisir usaha yang diperlukan untuk mengatur *environment* baru yang aman.
- Menghapus atau tidak menginstall fitur dan framework yang tidak digunakan.
- Meninjau dan memperbarui konfigurasi yang sesuai dengan standar keamanan.

- Menerapkan segmentasi antar komponen dengan segmentasi, containerization, atau cloud security groups (ACLs).
- Menerapkan *security headers.*
- Melakukan automasi untuk memverifikasi keefektifan dari konfigurasi dan setting di semua environments.

Revision #2
Created 2025-10-04 01:53:34 UTC by Tim Persandian
Updated 2025-10-04 03:00:53 UTC by Tim Persandian