A10:2021 - Server-Side Request Forgery

Deskripsi

Server-Side Request Forgery (SSRF) adalah jenis kerentanan keamanan yang terjadi ketika aplikasi web mengambil remote resource tanpa memvalidasi URL yang disediakan pengguna. Hal ini memungkinkan penyerang untuk memaksa aplikasi mengirimkan permintaan yang telah dimanipulasi ke tujuan yang tidak diharapkan, bahkan ketika aplikasi telah dilindungi oleh firewall, VPN, atau access control list (ACL) lainnya.

Dampak

- Penyerang dapat memaksa aplikasi untuk mengirim *crafted request* ke destinasi yang tidak diharapkan.
- Kebocoran data sensitif.
- Akses ke jaringan internal
- Serangan lateral dan eskalasi
- Gangguan / kerusakan sistem
- Pengungkapan infrastruktur dan arsitektur
- Pelanggaran kepatuhan

Mitigasi

- Melakukan segmentasi fungsionalitas akses ke remote resource dalam jaringan terpisah untuk mengurangi dampak SSRF.
- Menerapkan kebijakan firewall “deny by default” atau aturan kontrol akses jaringan yang hanya mengizinkan lalu lintas intranet penting.
- Sanitasi dan validasi semua data input pengguna.
- Menerapkan skema URL, port, dan tujuan dengan positive allow list.
- Menonaktifkan *HTTP redirections*.
- Perhatikan konsistensi URL untuk menghindari serangan seperti DNS rebinding dan kondisi race TOCTOU (time of check, time of use).
- Tidak mengembangkan layanan yang berhubungan dengan keamanan pada sistem yang berada di barisan depan,

- Khusus untuk *frontends* dengan pengguna/grup pengguna yang loyal atau berdedikasi serta dapat dikelola gunakanlah enkripsi jaringan (VPN) pada sistem independen mengingat adanya kebutuhan proteksi yang sangat tinggi.

Revision #1
Created 4 September 2024 04:31:18 by Tim Persandian
Updated 4 September 2024 04:37:23 by Tim Persandian