

A06:2021 - Vulnerable and Outdated Components

Deskripsi

Vulnerable and Outdated Components merupakan kerentanan perangkat lunak dalam aplikasi web yang memiliki celah keamanan atau tidak lagi mendapatkan dukungan berupa pembaruan atau *patch* dari pengembangnya. Komponen dapat mencakup *library*, *framework*, modul, atau bagian lain dari perangkat lunak yang digunakan dalam pengembangan aplikasi web.

Komponen yang tidak diperbarui dapat menjadi sasaran potensial bagi penyerang yang mencari celah keamanan untuk dieksploitasi. Kejadian ini terjadi antara lain karena:

- Komponen tersebut mungkin mempunyai bug atau celah keamanan yang telah diketahui dan dipublikasikan, tetapi belum diperbaiki.
- Tidak teridentifikasinya komponen yang digunakan secara langsung maupun dependensinya.
- Perangkat lunak rentan, tidak didukung, atau sudah usang.
- Tidak memindai kerentanan secara teratur terkait dengan komponen yang digunakan.
- Tidak memperbaiki atau mengupdate platform, kerangka kerja, dan dependensi yang digunakan.
- Tidak menguji kompatibilitas pustaka-pustaka yang diperbarui, ditingkatkan, atau di-patch.
- Tidak mengkonfigurasi komponen secara aman.

Dampak

Terdapat kerentanan/bug pada komponen yang dapat dieksploitasi

Mitigasi

- Menghapus dependensi, fitur, komponen, file, dan dokumentasi yang tidak digunakan.

- Inventarisasi versi komponen sisi klien dan sisi server secara terus menerus dan dependensinya
- Memantau secara terus menerus sumber-sumber informasi terkait kerentanan komponen seperti Common Vulnerability and Exposures (CVE) dan National Vulnerability Database (NVD) untuk kerentanan dalam komponen.
- Hanya mengunduh dan menginstal komponen dari sumber resmi melalui tautan yang aman. P
- Memantau pustaka dan komponen yang tidak dirawat atau tidak membuat patch keamanan untuk versi yang lebih lama.

Revision #1

Created 2025-10-04 03:02:00 UTC by Tim Persandian

Updated 2025-10-04 03:28:23 UTC by Tim Persandian