Metrik Ancaman (Threat Metrics)

Metrik ancaman (*threat metrics*) mengukur kondisi teknik eksploitasi / ketersediaan kode untuk mengeksploitasi kerentanan.

Metrik ancaman diukur berdasarkan kematangan eksploit / *exploit maturity* (E)

Kematangan Eksploit / Exploit Maturity (E)

Metrik mengukur kemungkinan serangan terhadap kerentanan berdasaekan kondisi eksploit saat ini, ketersediaan kode eksploit, atau aktif "in the wild". Ketersediaan eksploit untuk publik atau kemudahan instruksi penggunaan meningkatkan kemungkinan serangan, termasuk bagi penyerang yang tidak terampil. Ketersediaan eksploit atau instruksi juga dapat berkembang bergantung pada tingkat keberhasilan pembuktian eksploitasi kerentanan (*proof of concept*). Pada beberapa kasus, eksploitasi dapat dijalankan otomatis menggunakan tools serangan tertentu. Informasi terkait teknik eksploitasi / instruksi teknis lainnya selanjutnya akan disebut dengan intelijen ancaman (*threat intelligence*). Pada operasional organisasi disarankan menggunakan banyak sumber threat intelligence.

Daftar kemungkinan nilai kematangan eksploit ditunjukkan pada Tabel berikut.

Tabel. Kematangan Eksploit (Exploit Maturity)

Nilai Metrik	Deskripsi
Not Defined (X)	*Threat intelligence* yang handal tidak tersedia untuk menentukan karakteristik kematangan eksploitasi. Not Defined (X) merupakan nilai default.
Attacked (A)	Tersedia *threat intelligence:* melaporkan serangan terhadap percobaan / keberhasilan eksploitasi, atau terdapat tools untuk memudahkan eksploitasi kerentanan.
Proof of Concept (P)	Terdapat *threat intelligence*: pembuktian eksploitasi (*proof of concept*) dapat diakses publik, tidak terdapat laporan percobaan eksploitasi kerentanan, tidak terdapat pengetahuan /tools untuk memudahkan eksploitasi yang dapat diakses publik.

Unreported (U)	Terdapat *threat intelligence:* Tidak terdapat pembuktian eksploitasi (*proof of concept*) dapat diakses publik, tidak terdapat laporan percobaan eksploitasi kerentanan, tidak terdapat pengetahuan /tools untuk memudahkan eksploitasi yang dapat diakses publik.

Revision #4
Created 11 September 2024 04:17:00 by Tim Persandian
Updated 11 September 2024 07:23:33 by Tim Persandian