

Metrik Dampak (Impact Metrics)

Metrik menggambarkan dampak kerentanan yang berhasil dieksploitasi. Namun demikian, analis harus dapat menentukan batasan terhadap dampak akhir yang dapat dicapai oleh penyerang. Ketika mengidentifikasi nilai metrik dampak, perlu diperhitungkan dampak terhadap sistem yang rentan (*vulnerable system impact*) dan dampak diluar sistem yang rentan (*subsequent system impact*) yang ditentukan oleh dua hal yaitu dampak sistem rentan dan dampak selanjutnya yang muncul. Jika kerentanan tidak mempunyai dampak yang terjadi diluar sistem yang rentan, maka *subsequent metric* akan memiliki nilai NONE (N).

Metrik dampak terdiri atas beberapa kategori berikut.

Kerahasiaan / Confidentiality (VC/SC)

Metrik mengukur dampak kerahasiaan terhadap informasi karena keberhasilan eksploitasi kerentanan. Nilai dampak terhadap kerahasiaan ditunjukkan pada Tabel berikut.

Tabel. Metrik Dampak Kerahasiaan

Nilai Metrik	Dampak pada <i>Vulnerable System</i> (VC)	Dampak pada <i>Subsequent System</i> (SC)
High (H)	Semua informasi didalam sistem dapat diakses penyerang, atau akses terhadap informasi yang terbatas namun berdampak serius, misalnya kredensial sistem.	Semua informasi didalam <i>subsequent system</i> dapat diakses penyerang, atau akses terhadap informasi yang terbatas namun berdampak serius, misalnya kredensial sistem.
Low (L)	Penyerang dapat mengakses terhadap informasi terbatas, namun tidak memiliki kendali atas informasi tersebut sehingga tidak berdampak serius atau tidak menimbulkan kerugian secara langsung terhadap sistem.	Penyerang dapat mengakses terhadap informasi terbatas, namun tidak memiliki kendali atas informasi tersebut sehingga tidak berdampak serius atau tidak menimbulkan kerugian secara langsung terhadap <i>subsequent system</i> .
None (N)	Tidak terdapat informasi yang terungkap / hilang	Tidak terdapat informasi yang terungkap / hilang pada <i>subsequent system</i> .

Integritas / Integrity (VI/SI)

Metrik mengukur dampak integritas terhadap informasi karena keberhasilan eksploitasi kerentanan. Integritas sistem terdampak ketika penyerang dapat melakukan modifikasi terhadap data / informasi di dalam sistem. Nilai dampak terhadap integritas sistem ditunjukkan pada Tabel berikut.

Tabel. Metrik Dampak Integritas

Nilai Metrik	Dampak pada <i>Vulnerable System</i> (VC)	Dampak pada <i>Subsequent System</i> (SC)
High (H)	Hilangnya perlindungan integritas sistem. Penyerang dapat memodifikasi seluruh file yang dilindungi didalam sistem, atau hanya dapat melakukan modifikasi pada file tertentu, namun modifikasi yang berbahaya dapat berdampak serius pada sistem.	Hilangnya perlindungan integritas sistem. Penyerang dapat memodifikasi seluruh file yang dilindungi didalam sistem, atau hanya dapat melakukan modifikasi pada file tertentu, namun modifikasi yang berbahaya dapat berdampak serius pada <i>subsequent system</i> .
Low (L)	Penyerang dapat melakukan modifikasi, namun tidak memiliki kendali atas akibat dari modifikasi tersebut atau jumlah modifikasi dibatasi sehingga tidak berdampak serius atau tidak menimbulkan kerugian secara langsung terhadap sistem.	Penyerang dapat melakukan modifikasi, namun tidak memiliki kendali atas akibat dari modifikasi tersebut atau jumlah modifikasi dibatasi sehingga tidak berdampak serius atau tidak menimbulkan kerugian secara langsung terhadap <i>subsequent system</i> .
None (N)	Tidak terdapat integritas sistem yang hilang.	Tidak terdapat integritas <i>subsequent system</i> yang hilang.

Ketersediaan / Availability (VA/SA)

Metrik mengukur dampak ketersediaan terhadap informasi karena keberhasilan eksploitasi kerentanan. Ketersediaan sistem terdampak ketika penyerang dapat mengganggu ketersediaan akses / membuat sistem tidak dapat diakses oleh pengguna. Nilai dampak terhadap ketersediaan sistem ditunjukkan pada Tabel berikut.

Tabel. Metrik Dampak Ketersediaan

Nilai Metrik	Dampak pada <i>Vulnerable System</i> (VC)	Dampak pada <i>Subsequent System</i> (SC)
--------------	---	---

High (H)	Hilangnya perlindungan ketersediaan sistem. Penyerang dapat menolak seluruh akses kedalam sistem, baik bersifat sementara maupun terus menerus (persistent). Atau penyerang dapat menolak beberapa akses, namun berdampak serius terhadap ketersediaan sistem.	Hilangnya perlindungan ketersediaan layanan <i>subsequent system</i> . Penyerang dapat menolak seluruh akses kedalam <i>subsequent system</i> , baik bersifat sementara maupun terus menerus (persistent). Atau penyerang dapat menolak beberapa akses, namun berdampak serius terhadap ketersediaan <i>subsequent system</i> .
Low (L)	Terdapat gangguan terhadap ketersediaan sistem, namun tidak dapat sepenuhnya menolak layanan kepada pengguna yang sah.	Terdapat gangguan terhadap ketersediaan layanan <i>subsequent system</i> , namun tidak dapat sepenuhnya menolak layanan kepada pengguna yang sah.
None (N)	Tidak terdapat gangguan terhadap ketersediaan sistem .	Tidak terdapat gangguan terhadap ketersediaan <i>subsequent system</i>

Revision #8

Created 5 September 2024 03:04:01 by Tim Persandian

Updated 11 September 2024 04:18:11 by Tim Persandian