**Nama : Ulviyana**

**Nim : 09011281520090**

**CVE** adalah singkatan dari *Common Vulnerability and Exposure.* Dalam keamanan informasi, **Vulnerability** adalah sebuah software coding error yang digunakan oleh peretas untuk masuk ke sebuah sistem informasi dan melakukan aktivitas yang tidak sah dengan menyamar sebagai pengguna yang berwenang. Sedangkan **Exposure** adalah sebuah software error yang memungkinkan peretas masuk ke sistem penyerang dapat memperoleh informasi atau menyembunyikan tindakan yang tidak sah.

Tujuan utama CVE adalah berbagi data tentang vulnerabiities dan exposure yang sudah pernah terjadi diberbagai database dan menjelaskan apa dampaknya. Sehingga CVE membantu vendor keamanan komputer untuk mengidentifikasikan vulnerabilities dan exposures.

Salah satu CVE yang terdaftar adalah CVE-2017-8733. CVE-2017-8733 memungkinkan peretas untuk mendapatkan informasi yang sensitif via web site palsu, atau yang biasa disebut "Internet Explorer Spoofing Vulnerability."Ini akan memungkinkan penyerang untuk mengelabui pengguna agar menjadi percaya bahwa pengguna tersebut mengunjungi situs web yang sah, karena cara Internet Explorer menangani konten HTML tertentu.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| |  | | --- | | Referensi CVE :   [CVE-2017-8733](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-8733" \t "_blank), [CVE-2017-8747](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-8747), [CVE-2017-8749](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-8749) | | Tanggal :  Sep 12 2017 | | Dampak: Pengungkapan informasi pengguna, Pelaksanaan kode sewenang-wenang melalui jaringan, Modifikasi informasi pengguna, dan Akses pengguna melalui jaringan. | | Berikut keterangan dari pihak Masato Kinugawa dari Cure53 dan Hui Gao dari Palo Alto Networks yang melaporkan adanya kerentanan seperti berikut ini :   * Beberapa kerentanan dilaporkan terjadi di Microsoft Internet Explorer, penyerang dapat menyebabkan kode sewenang-wenang yang dieksekusi pada sistem pengguna, dan penyerang bisa menipu server. * Penyerang dapat membuat konten yang dibuat khusus, yang saat dimuat oleh pengguna, akan memicu kesalahan pemrosesan HTML dan konten web spoof. * Penyerang dapat membuat konten yang dibuat khusus, yang saat dimuat oleh pengguna, akan memicu kesalahan penanganan memori objek dan mengeksekusi kode sewenang-wenang pada sistem pengguna. | | Adapun dari keterangan di atas menyebabkan dampak seperti berikut ini:  Penyerang dapat membuat konten yang jika dimuat oleh pengguna akan mengeksekusi kode sewenang-wenang pada sistem pengguna. Penyerang bisa menipu konten.  Solusi :  Vendor telah mengeluarkan perbaikan. | |  | |

**How to attack**:

*Web Spoofing* melibatkan sebuah server web yang dimiliki penyerang yang diletakkan pada internet antara pengguna dengan WWW, sehingga akses ke web yang dituju pengguna akan melalui server penyerang. Cara seperti ini dikenal dengan sebutan “man in the middle attack. Hal ini dapat terjadi dengan beberapa jalan, tapi yang paling mungkin adalah :

* Akses ke situs web diarahkan melalui sebuah *proxy server* : ini disebut (HTTP)*application proxy*. Hal ini memberikan pengelolaan jaringan yang lebih baik untuk akses ke server. Ini merupakan teknik yang cukup baik yang digunakan pada banyak situs-situs di internet, akan tetapi teknik ini tidak mencegah *Web Spoofing*.
* Seseorang menaruh link yang palsu (yang sudah di-*hack*) pada halaman web yang populer.
* Kita menggunakan browser mengakses sebuah Web. Semua yang ada pada NET (baik Internet maupun Intranet) direferensikan dengan Universal Resource Loactor (URL). Pertama-tama penyerang harus menulis ulang URL dari halaman web yang dituju sehingga mereka mengacu ke server yang dimiliki penyerang daripada ke server web yang sebenarnya. Misalnya, server penyerang terletak di [www.attacler.com](http://www.attacler.com), maka penyerang akan menulis ulang URL dengan menambahkan htpp://www.attacker.com didepan URL yang asli.