

Tugas Keamanan Jaringan Komputer

Five Common Vulnerabilities and Exposures Dos Attack in Windows

Server 2008



Nama : Aidil Fitri Yansya

NIM : 09011281419054

Kelas : SK8 PIL

Dosen Pembimbing : Deris Stiawan, M.T., Ph.D

**JURUSAN SISTEM KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS SRIWIJAYA**

Vulnerability Details : CVE-2017-11788

Windows Search Object Memory Handling Error Lets Remote Users Deny Service

Deskripsi: Kerentanan dilaporkan di Windows Search. Pengguna jarak jauh dapat menyebabkan penolakan kondisi layanan pada sistem target. Seorang pengguna jarak jauh dapat mengirim pesan yang dibuat secara khusus ke layanan pencarian Windows yang ditargetkan untuk memicu kesalahan penanganan memori objek dan menyebabkan penolakan terhadap kondisi layanan. Ini juga bisa dimanfaatkan oleh remote user melalui koneksi SMB.

Impact: A remote user can cause denial of service conditions.

Vulnerability Details : CVE-2015-6112

Windows Schannel TLS Implementation Lets Remote Users Spoof Servers

Deskripsi : Kerentanan dilaporkan terjadi di Windows Schannel. Pengguna jarak jauh bisa menipu server. Pengguna jarak jauh yang bisa melakukan serangan man-in-the-middle antara target client dan server bisa menipu server.

Impact : A remote user can spoof a server.

Vulnerability Details : CVE-2015-0095

Windows Kernel-Mode Driver Bugs Let Local Users Obtain Potentially Sensitive Information and Gain Elevated Privileges

Deskripsi : Beberapa kerentanan dilaporkan terjadi pada Windows Kernel-Mode Driver. Pengguna lokal dapat memperoleh hak istimewa yang tinggi pada sistem target. Pengguna lokal dapat memperoleh informasi yang berpotensi sensitif. Driver mode kernel tidak menginisialisasi buffer fungsi dengan benar [CVE-2015-0077]. Pengguna lokal dapat memanfaatkan ini untuk mendapatkan kredensial administratif.

Vulnerability Details : CVE-2012-2551

Microsoft Kerberos Null Pointer Dereference Lets Remote Users Deny Service

Deskripsi : Kerentanan dilaporkan terjadi di Microsoft Kerberos. Pengguna jarak jauh dapat menyebabkan penolakan terhadap kondisi layanan. Seorang pengguna jarak jauh dapat mengirim data yang dibuat khusus untuk memicu dereferensi pointer nol dan menyebabkan server Kerberos target berhenti merespons dan restart.

Vulnerability Details : CVE-2012-0006

Microsoft DNS Server Lets Remote Users Deny Service

Deskripsi : Kerentanan dilaporkan di Microsoft DNS Server. Pengguna jarak jauh dapat menyebabkan penolakan terhadap kondisi layanan. Pengguna jarak jauh dapat mengirim kueri DNS yang dibuat secara khusus sehingga sistem target berhenti merespons dan restart secara otomatis. Kerentanan berada dalam pengelolaan objek dalam memori sementara sistem mencari catatan sumber daya.

Impact: A remote user can cause the target system to stop responding and automatically restart.

Analisis

Dari 5 common vulnerabilities and exposures diatas saya memilih serangan dos pada windows server 2008 untuk dianalisis. Berdasarkan data diatas menjelaskan bahwa Pengguna jarak jauh dapat menyebabkan penolakan kondisi layanan pada sistem target, CVE tersebut juga menjelaskan mengenai penggunaan jarak jauh terhadap target client dan Server. Pengguna lokal dapat memperoleh informasi yang berpotensi sensitif. Dampak yang dihasilkan dari CVE tersebut user dapat menyebabkan system target terhenti merespons dan merestart secara otomatis, Penggunaan jarak jauh dapat mengeksploitasi server, Pengguna jarak jauh dapat menyebabkan penolakan terhadap kondisi layanan.