Tugas Keamanan Jaringan Komputer

Common Vulnerabilities and Exposures

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

Windows Server 2008

Windows Server 2008 adalah nama sistem operasi untuk server dari perusahaan Microsoft. Sistem server ini merupakan pengembangan dari versi sebelumnya yang disebut Windows Server 2003. Pada tanggal 15 Mei 2007, Bill Gates mengatakan pada konferensi WinHEC bahwa Windows Server 2008 adalah nama baru dari *Windows Server "Konciiiii".*

Windows Server 2008 mendukung sistem klien dengan Windows Vista, mirip seperti hubungan antara *Windows Server 2003* dan Windows XP. Versi Beta 1 dari sistem server ini pertama kali dikenalkan pada tanggal 27 Juli 2005, dan versi Beta 3-nya sudah diumumkan pada tanggal 25 April 2007 yang lalu. Produk ini rencananya akan dipasarkan pada pertengahan kedua tahun 2007 ini. Windows Server 2008 adalah nama sistem operasi untuk server dari perusahaan Microsoft. Sistem server ini merupakan pengembangan dari versi sebelumnya yang disebut Windows Server 2003.

Fitur

Windows Server 2008 dibangun dari kode yang sama seperti Windows Vista; karenanya Windows Server 2008 memiliki arsitektur dan fungsionalitas yang sama dengannya. Karena Windows Vista, oleh Microsoft, menawarkan kemajuan secara teknis dibandingkan dengan Windows versi sebelumnya, maka hal-hal yang dimiliki oleh Windows Vista juga dimiliki oleh Windows Server 2008. Dari sisi perangkat keras, prosesor dan perangkat memori dimodelkan sebagai perangkat keras Plug and Play, sehingga mengizinkan proses *hot-plugging* terhadap perangkat-perangkat tersebut. Ini berarti, sumber daya sistem dapat dibagi ke dalam partisi-partisi secara dinamis dengan menggunakan fitur *Dynamic Hardware Partitioning*, di mana setiap partisi memiliki memori, prosesor, I/O secara independen terhadap partisi lainnya.

Berdasarkan dengan pembahasan diatas, saya mengambil contoh website : www.pertamina.com yang menggunakan windows server 2008 sebagai OS dan web servernya : Microsoft-IIS/10.0, saya mendapatkan info melalui website www.netcraft.com .

	Site	Site Report	First seen	Netblock	OS
1.	www.pertamina.com		september 1996	indosatm2 idc jatipadang allocation	windows server 2008
2.	recruitment.pertamina.com		november 2012	indosatm2 idc jatipadang allocation	windows server 2008

Hosting History

Netblock owner	IP address	OS	Web server	Last seen Refresh
Microsoft Corporation One Microsoft Way Redmond WA US 98052	52.163.122.160	unknown	Microsoft-IIS/10.0	19-Feb-2018
INDOSATM2 IDC Jatipadang Allocation Jl. Kebagusan raya No 36 Ragunan, Jakarta Selatan Indonesia	219.83.125.163	unknown	unknown	21-Feb-2017
INDOSATM2 IDC Jatipadang Allocation Jl. Kebagusan raya No 36 Ragunan, Jakarta Selatan Indonesia	219.83.125.163	unknown	Microsoft-IIS/7.5	13-Oct-2013
SoftLayer Technologies Inc. 1950 N Stemmons Freeway Dallas TX US 75207	75.126.36.10	Windows Server 2003	Microsoft-IIS/6.0	31-May-2012
SoftLayer Technologies Inc. 1950 N Stemmons Freeway Dallas TX US 75207	75.126.36.10	Windows Server 2003	Microsoft-IIS/6.0	1-Aug-2007
SoftLayer Technologies Inc. 1950 N Stemmons Freeway Dallas TX US 75207	75.126.36.10	Windows Server 2003	Microsoft-IIS/6.0	20-Dec-2006
SoftLayer Technologies Inc. 1950 N Stemmons Freeway Dallas TX US 75207	69.56.139.168	Windows Server 2003	-	28-Jul-2006
SoftLayer Technologies Inc. 1950 N Stemmons Freeway Dallas TX US 75207	69.56.139.168	Windows Server 2003	Microsoft-IIS/6.0	4-Jun-2006
SoftLayer Technologies Inc. 1950 N Stemmons Freeway Dallas TX US 75207	69.56.139.168	unknown	Microsoft-IIS/6.0	17-Apr-2006
SoftLayer Technologies Inc. 1950 N Stemmons Freeway Dallas TX US 75207	69.56.139.168	Windows Server 2003	Microsoft-IIS/6.0	19-Jul-2004

Berdasarkan info yang didapat dari penjelasan diatas IP yang digunakan oleh pertamina.com ialah 52.163.122.160 untuk yang terakhir di update pada tanggal 19-Februari-2018. Untuk mencari celah keamanan nya menggunakan CVE yaitu Common Vulnerabilities and Exposures

CVE adalah kamus cyber security yang diketahui untuk kerentanan umum. Tujuan: Mengidentifikasi dan memberi nama secara terbuka kepada umum kerentanan yang berkaitan dengan versi perangkat lunak tertentu atau code bases.

Hole yang akan dibahas ialah mengenai :

Vulnerabilities in Windows OLE Could Allow Remote Code Execution (3011443)

– CVSS Scores & Vulnerability Types

CVSS Score	9.3
Confidentiality Impact	Complete (There is total information disclosure, resulting in all system files being revealed.)
Integrity Impact	Complete (There is a total compromise of system integrity. There is a complete loss of system protection, resulting in the entire system being compromised.)
Availability Impact	Complete (There is a total shutdown of the affected resource. The attacker can render the resource completely unavailable.)
Access Complexity	Medium (The access conditions are somewhat specialized. Some preconditions must be satistified to exploit)
Authentication	Not required (Authentication is not required to exploit the vulnerability.)
Gained Access	None
Vulnerability Type(s)	Execute Code
CWE ID	94

Hole tersebut memungkinkan penyerang jarak jauh untuk mengeksekusi kode sewenang-wenang melalui situs web yang dibuat, seperti yang ditunjukkan oleh sebuah upaya redimensioning array yang memicu penanganan nilai suatu fungsi SafeArrayDimen yang tidak semestinya, alias Windows OLE Automation Array Remote Code Execution Vulnerability.

Pembaruan keamanan ini memecahkan dua kerentanan yang dilaporkan secara pribadi di Microsoft Windows Object Linking and Embedding (OLE). Yang paling parah dari kerentanan ini memungkinkan eksekusi kode jauh jika pengguna melihat halaman web yang dibuat secara khusus menggunakan Internet Explorer. Seorang penyerang yang berhasil mengeksploitasi kerentanan bisa menjalankan kode sewenang-wenang dalam konteks pengguna saat ini. Jika pengguna saat ini masuk dengan hak pengguna administratif, penyerang kemudian dapat menginstal program; melihat, mengubah, atau menghapus data; atau buat akun baru dengan hak pengguna penuh. Pelanggan yang akunnya dikonfigurasi agar lebih sedikit hak pengguna di sistem dapat kurang terpengaruh daripada pengguna yang beroperasi dengan hak pengguna administratif.

Pembaruan keamanan ini dinilai Kritis untuk semua edisi Microsoft Windows yang didukung. Untuk informasi lebih lanjut, lihat bagian Perangkat Lunak yang Terkena Dampak.

Pembaruan keamanan membahas kerentanan dengan memodifikasi bagaimana sistem operasi yang terpengaruh memvalidasi penggunaan memori saat objek OLE diakses, dan dengan memodifikasi bagaimana Internet Explorer menangani objek di memori. Untuk informasi lebih lanjut tentang kerentanan, lihat Bagian Pertanyaan yang Sering Diajukan (FAQ) untuk kerentanan spesifik.

Pembaruan keamanan ini juga membahas kerentanan yang pertama kali dijelaskan di Microsoft Security Advisory 3010060.

How to Attack

Title : Microsoft Windows HTA (HTML Application) - Remote Code Execution
Tested on Windows 7 / Server 2008
Author : Mohammad Reza Espargham

MS14-064

Step How to Attack Microsoft Windows HTA (HTML Application) - Remote Code Execution

1 . run php code : php hta.php
2 . copy this php output (HTML) and Paste as poc.hta (Replace ip)
3 . open poc.hta
4 . Your Link Download/Execute on your target
5 . Finished ;)

Analisis Hole

Kerusakan eksekusi kode jarak jauh ada saat Internet Explorer tidak benar mengakses objek di memori. Microsoft menerima informasi tentang kerentanan ini melalui pengungkapan kerentanan terkoordinasi. Saat buletin keamanan ini dikeluarkan, Microsoft belum menerima informasi apapun untuk menunjukkan bahwa kerentanan ini telah umum digunakan untuk menyerang pelanggan. Pembaruan ini membahas kerentanan dengan memodifikasi cara sistem operasi yang terpengaruh memvalidasi penggunaan memori saat objek OLE diakses, dan dengan memodifikasi cara Internet Explorer menangani objek dalam memori