TUGAS KEAMANAN JARINGAN KOMPUTER

Nama : M. Atma Utama Septiando

NIM : 09011281419052

Kelas : SK8P

Jurusan : Sistem Komputer

Fakultas : Ilmu Komputer

Universitas Sriwijaya

CVE pada WINDOWS :

CVE ID : CVE-2015-1635

Deskripsi :

HTTP.sys di Microsoft Windows 7 SP1, Windows Server 2008 R2 SP1, Windows 8, Windows 8.1, dan Windows Server 2012 Gold dan R2 memungkinkan penyerang jarak jauh melakukan kode sewenang-wenang melalui permintaan HTTP yang dibuat, alias "HTTP.sys Remote Code Execution Vulnerability. "

Microsoft Windows HTTP Protocol Stack CVE-2015-1635 Remote Code Execution Vulnerability :

Bugtraq ID	:	74013
Class	:	Design Error
CVE	:	CVE-2015-1635
Remote	:	Yes
Local	:	No
Published	:	Apr 14 2015 12:00AM
Updated	:	Aug 10 2017 06:10PM
Credit	:	Citrix Security Response Team
Vulnerable	:	Siemens SPECT/CT Systems 0 Siemens SPECT Workplaces/Symbia.net 0 Siemens SPECT Systems 0 Siemens PET/CT Systems 0 Microsoft Windows Server 2012 R2 0 Microsoft Windows Server 2012 0 Microsoft Windows Server 2008 R2 for x64-based Systems SP1 Microsoft Windows Server 2008 R2 for Itanium-based Systems SP1 Microsoft Windows 8 for x64-based Systems 0 Microsoft Windows 8 for 32-bit Systems 0 Microsoft Windows 7 for x64-based Systems SP1 Microsoft Windows 7 for 32-bit Systems SP1 Avaya Meeting Exchange - Webportal 6.2 Avaya Meeting Exchange - Webportal 6.0 Avaya Meeting Exchange - Webportal 5.2.1 Avaya Meeting Exchange - Webportal 5.2 Avaya Meeting Exchange - Webportal 5.0.1 Avaya Meeting Exchange - Webportal 5.0 Avaya Meeting Exchange - Web Conferencing Server 6.2 Avaya Meeting Exchange - Web Conferencing Server 6.0 Avaya Meeting Exchange - Web Conferencing Server 5.2.1 Avaya Meeting Exchange - Web Conferencing Server 5.2 Avaya Meeting Exchange - Web Conferencing Server 5.0.1 Avaya Meeting Exchange - Web Conferencing Server 5.0 Avaya Meeting Exchange - Streaming Server 6.2 Avaya Meeting Exchange - Streaming Server 6.0

Avaya Meeting Exchange - Streaming Server 5.2.1
Avaya Meeting Exchange - Streaming Server 5.2
Avaya Meeting Exchange - Streaming Server 5.0.1
Avaya Meeting Exchange - Streaming Server 5.0
Avaya Meeting Exchange - Recording Server 6.2
Avaya Meeting Exchange - Recording Server 6.0
Avaya Meeting Exchange - Recording Server 5.2.1
Avaya Meeting Exchange - Recording Server 5.2
Avaya Meeting Exchange - Recording Server 5.0.1
Avaya Meeting Exchange - Recording Server 5.0
Avaya Meeting Exchange - Client Registration Server 6.2
Avaya Meeting Exchange - Client Registration Server 6.0
Avaya Meeting Exchange - Client Registration Server 5.2.1
Avaya Meeting Exchange - Client Registration Server 5.2
Avaya Meeting Exchange - Client Registration Server 5.0.1
Avaya Meeting Exchange - Client Registration Server 5.0

How to Attack :

Produk keamanan Symantec mencakup database signature serangan yang ekstensif. Signature serangan adalah pengaturan informasi unik yang dapat digunakan untuk mengidentifikasi upaya penyerang untuk mengeksploitasi sistem operasi atau kerentanan aplikasi yang diketahui. Saat Intrusion Detection mendeteksi tanda tangan serangan, ini akan menampilkan Security Alert.

Saat ini, produk keamanan Symantec memantau eksploitasi ini:

Adobe Reader GetIcon BO, Backdoor C.I.A, Web Attack: Facebook Malicious Permission Request, W32 Beagle A Worm Backdoor, dsb.

- Keparahan: Tinggi

Serangan ini bisa menimbulkan ancaman keamanan serius. Anda harus segera melakukan tindakan untuk menghentikan kerusakan atau mencegah kerusakan lebih lanjut terjadi.

- Deskripsi

Tanda tangan ini mendeteksi upaya untuk mengeksploitasi kerentanan eksekusi kode jarak jauh pada Microsoft Windows.

- Informasi tambahan

Microsoft Windows rentan terhadap kerentanan eksekusi kode jarak jauh karena gagal mengurai permintaan HTTP yang dibuat dengan benar. Secara khusus, masalah ini terjadi pada tumpukan protokol HTTP 'HTTP.sys'. Penyerang dapat memanfaatkan masalah ini dengan mengirimkan permintaan HTTP yang dibuat secara khusus.

Seorang penyerang dapat memanfaatkan masalah ini untuk mengeksekusi kode sewenang-wenang dalam konteks akun sistem. Kegagalan usaha eksploitasi kemungkinan akan berakibat pada kondisi denial-of-service.

- Mempengaruhi :

Microsoft Windows Server 2008 R2 untuk Sistem x64 berbasis SP1
Microsoft Windows 7 untuk Sistem x64 berbasis SP1
Microsoft Windows 7 untuk Sistem 32-bit SP1