KEAMANAN JARINGAN KOMPUTER

Marini Suprianty

(09011181419016)

FAKULTAS ILMU KOMPUTER

JURUSAN SISTEM KOMPUTER

UNIVERSITAS SRIWIJAYA

TUGAS 2

FITUR

	Site	Site Report	First seen	Netblock	OS
1.	go.microsoft.com		november 2001	akamai technologies	linux
2.	www.microsoft.com		august 1995	akamai international, bv	linux
3.	support.microsoft.com		october 1997	akamai international, bv	linux
4.	download.microsoft.com		august 1999	akamai international, bv	linux
5.	technet.microsoft.com		august 1999	microsoft corporation	windows server 2012
6.	msdn.microsoft.com		september 1998	microsoft corporation	windows server 2012
7.	answers.microsoft.com		august 2009	akamai international, bv	linux
8.	www.catalog.update.microsoft.com		december 2016	microsoft corporation	windows server 2016
9.	windows.microsoft.com		june 1998	akamai international, bv	linux
10.	social.technet.microsoft.com		august 2008	microsoft corporation	windows server 2012
11.	catalog.update.microsoft.com		october 2007	microsoft corporation	windows server 2008
12.	o15.officeredir.microsoft.com		may 2012	microsoft corporation	windows server 2016
13.	office.microsoft.com		november 1998	microsoft corp	unknown
14.	e.microsoft.com		january 2014	microsoft informatica ltda	f5 big-ip
15.	azure.microsoft.com		may 2014	microsoft informatica ltda	windows server 2012
16.	www.microsoftstore.com		november 2008	akamai international, bv	linux
17.	www.microsofttranslator.com		november 2008	microsoft corporation	windows server 2012
18.	microsoft.com		may 1996	microsoft corporation	windows server 2012
19.	www.update.microsoft.com		may 2007	microsoft corporation	windows server 2012
20.	login.microsoftonline.com		december 2010	microsoft corporation	windows server 2012

Terlihat pada gambar di atas bahwa website dari Microsoft menggunakan sistem Operasi Linux dan windows server, penjelasan sebagai berikut.

Linux

Linux adalah sistem operasi berbasis Unix yang dibuat oleh Linus Torvalds, dikembangkan oleh GNU General Public License. Linux bersifat open-source atau bebas digunakan atau didownload oleh pengguna komputer diseluruh dunia atau juga disebut dengan istilah FOSS (Free / Open Source Software).

Ada bermacam-macam fitur pada Sistem Operasi Linux. Fitur-fitur sistem operasi Linux adalah :

- Multitasking : Beberapa proses dalam dijalankan pada suatu saat.
- Multiuser : Beberapa user di mesin yang sama pada suatu saat.
- Multiplatform : Sistem operasi Linux berjalan di banyak CPU berbeda.
- Multiprocessor : Mendukung SMP (Symmentric Multiprocessing) untuk intel dan SPARC dan platform lain.
- Mode Protected : Berjalan pada mode proteceted intel x86.
- Memenuhi IEEE POSIX.1 : Linux kompatibel dengan banyak standar UNIX di tingkat kode sumber, IEEE POSIX.1 serta fitur-fitur system V dan BSD.

- Proteksi Memori : Mempunyai proteksi memori sehingga bug di satu program tidak menyebabkan seluruh program down.
- Demand Page Loaded Executable : Mengimplementasikan demand paging loading executable.
- Shared Copy on Write Pages Antara Executables : Banyak proses dapat menggunakan memori yang sama. Saat satu program mencoba menulis memori tersebut. Page (4 Kb memori) yang berbeda ini baru disalin ke suatu tempat.
- Virtual Memori : Virtual memori menggunakan sistem paging (disk-paging).
- Unified Memori Pool : Mengimplementasikan unified memori pool untuk program disk chace.
- Dynamically Linked Share Libraries : Mengimplementasikan dynamically linked share libraries.
- Post-Mortem Analysis untuk Debugging : Memungkinkan menggukan debugger pada program tidak hanya selama program berjalan tapi juga setelah program mengalami crash.
- iBCS2 (iBCS2-complaint emulation module) : Dengan modul emulasi yang memenuhi iBCS2, kebanyakkan kompatibel dengan SCO,SVR3 dan SVR4 di tingkat biner.
- Kode Sumber Bebas : Semua kode sumber yang ada tersedia, termasuk kernel dan driver, sehingga memudahkan pengembangan program user.
- POSIX Job Control : Digunakan pada shell csh dan bash.
- Customized-Keyboard : Mendukung keyboard dari berbagai negara.
- Multiple Virtual Consoles : Beberapa sesi login independen dengan konsol.
- Mendukung Beragam File System : Hampir semua file system dapat diimplementasikan.
- Pengaksesan Transparan ke Partisi MS-DOS : Untuk mengakses partisi MS-DOS tidak dibutuhkan sistem file khusus dan juga tidak memerlukan perintah khusus untuk menggunakan partisi MS-DOS.
- Sistem File UMSDOS memungkinkan Linux di install pada MS-DOS.
- Implementasi TCP/IP Networking : Untuk jaringan TCP/IP cukup lengkap.
- Mendukung sistem file HPFS-2 read only untuk OS/2.
- Mendukung sistem file HFS (Macintosh) sebagai modul terpisah.
- Dapat membaca sistem file CD-ROM : Bisa membaca file-file yang beranekaragam yang disimpan di CD-ROM.
- Terdapat pada Apple Talk Server.
- Dapat sebagai Netware Client dan berhubungan dengan Netware Server.
- Dapat sebagai LAN Manager Client.
- Protocol jaringan cukup lengkap.

Dan selain fitur yang digunakan, pada website unpad.ac.id terdapat masing masing lis yang berisikan data data CVE yang digunakan untuk melihat security hole pada tiap domain. Berikut penjelasannya’

Windows Server 2012

Fitur yang disediakan oleh Microsoft Windows Server adalah untuk kepentingan server yang akan kita gunakan, tergantung kita yang menggunakan, artinya kita tidak perlu menggunakan seluruh fitur yang ada sekaligus dalam 1 PC, itu akan lebih mengurangi performance daripada server yang kita jalankan. Saran saya gunakan satu persatu fitur pada 1 PC, seperti pada kita akan membuat DNS server pada PC 1, dan untuk web server pada PC 2 ini akan lebih meningkatkan performance server kita.

Fitur yang ada di Windows Server yang sering digunakan antara lain adalah dua yang disebutkan tadi yaitu DNS Server dan web server (Internet Information Server) atau sering disebut dengan IIS. Selain dua ini, yangn sangat perperan penting adalah pada Active Directory (AD).

Fungsi DNS yaitu sebagai translator yang menangani request dengan nama terentu ke IP si penyedia. Misalkan anda punya website atau blog yang anda tanam ke komputer dengan IP 192.168.1.2 nah, DNS ini dapat membuatkan nama dari IP tersebut seperti contoh www.websayaa.tes. nama domain www.websayaa.tes ini ketika di buka oleh seseorang atau dibuka oleh semua orang ia akan langsung mencari dengan alamat IP 192.168.1.2 tadi yaitu IP yang memuat websitenya dan kemudian ia akan mengembalikan request tersebut dengan membukakan website nya di IP tersebut.

Common Vuralrabilities and Exposures

CVE (Common Vulnerabilities and Exposures) adalah kamus dari nama standar untuk kerentanan dan eksposur keamanan informasi lainnya, yang telah diadopsi oleh sejumlah besar organisasi di seluruh industri keamanan komputer. Nama CVE sering dikutip dalam advisori keamanan.

Nama CVE untuk setiap kerentanan disertakan sebagai bagian dari informasi untuk setiap kerentanan dalam laporan. Dalam laporan online yang dihasilkan oleh Netcraft, nama CVE termasuk dalam kolom "CVE name" di tabel kerentanan. Dalam laporan "dapat dicetak", nama CVE disertakan dalam tanda kurung setelah deskripsi kerentanan. Anda dapat mencari laporan untuk nama CVE tertentu dengan menggunakan kemampuan pencarian teks pada browser.

Network

Site	http://www.microsoft.com	**Netblock Owner**	Akamai International, BV
Domain	microsoft.com	**Nameserver**	ns1.msft.net
IP address	23.200.101.224	**DNS admin**	msnhst@microsoft.com
IPv6 address	2a02:26f0:71:4a0:0:0:0:356e	**Reverse DNS**	a23-200-101-224.deploy.static.akamaitechnologies.com
Domain registrar	*unknown*	**Nameserver organisation**	*unknown*
Organisation	*unknown*	**Hosting company**	Akamai Technologies
Top Level Domain	Commercial entities (.com)	**DNS Security Extensions**	*unknown*
Hosting country	NL	**Latest Performance**	Performance Graph

Hosting History

Netblock owner	IP address	OS	Web server	Last seen Refresh
Akamai International, BV Prins Bernhardplein 200 Amsterdam NL 1097 JB	23.195.133.197	Linux	unknown	18-Feb-2018
Akamai Technologies	2.19.152.139	Linux	unknown	17-Feb-2018
Akamai International, BV Prins Bernhardplein 200 Amsterdam NL 1097 JB	23.60.196.55	Linux	unknown	9-Feb-2018
Akamai International, BV Prins Bernhardplein 200 Amsterdam NL 1097 JB	104.82.99.6	Linux	unknown	6-Feb-2018
Akamai International, BV Prins Bernhardplein 200 Amsterdam NL 1097 JB	23.195.133.197	Linux	unknown	30-Jan-2018
Akamai International, BV Prins Bernhardplein 200 Amsterdam NL 1097 JB	184.28.56.211	Linux	unknown	23-Jan-2018
Akamai	88.221.16.103	Linux	unknown	21-Jan-2018
Akamai International, BV Prins Bernhardplein 200 Amsterdam NL 1097 JB	184.28.56.211	Linux	unknown	14-Jan-2018
Akamai International, BV Prins Bernhardplein 200 Amsterdam NL 1097 JB	23.44.100.111	Linux	unknown	10-Jan-2018
Akamai International, BV Prins Bernhardplein 200 Amsterdam NL 1097 JB	23.212.232.92	Linux	unknown	7-Jan-2018

Pada gambar diatas terlihat bahwa Microsoft.com dengan IP 104.82.166.224 yang menggunakan Linux sebagai sistem operasi dan Nginx sebagai webserverny. itu merupakan upgrade terakhir webserver yang digunakan oleh Microsoft.com pada tahun 2018.

DNS Records for microsoft.com

Name	TTL	Class	Type	Priority	Data
microsoft.com.	3600	IN	SOA		ns1.msft.net. msnhst.microsoft.com. 2018021906 7200 600 2419200 3600
microsoft.com.	172800	IN	NS		ns4.msft.net.
microsoft.com.	172800	IN	NS		ns1.msft.net.
microsoft.com.	172800	IN	NS		ns2.msft.net.
microsoft.com.	172800	IN	NS		ns3.msft.net.
microsoft.com.	3600	IN	A		23.96.52.53
microsoft.com.	3600	IN	A		191.239.213.197
microsoft.com.	3600	IN	A		104.40.211.35
microsoft.com.	3600	IN	A		104.43.195.251
microsoft.com.	3600	IN	A		23.100.122.175
microsoft.com.	3600	IN	TXT		"facebook-domain-verification=gx5s19fp3o8aczby6a22clfhzm03as"
microsoft.com.	3600	IN	TXT		"google-site-verification=6P08Ow5E-8Q0m6vQ7FMAqAYIDprkVV8fUf_7hZ4Qvc8"
microsoft.com.	3600	IN	TXT		"facebook-domain-verification=m54hfzczreqq2z1pf99y2p0kpwwpkv"
microsoft.com.	3600	IN	TXT		"v=spf1 include:_spf-a.microsoft.com include:_spf-b.microsoft.com include:_spf-c.microsoft.com include:_spf-ssg-a.microsoft.com include:spf-a.hotmail.com ip4:147.243.128.24 ip4:147.243.128.26 ip4:147.243.1.153 ip4:147.243.1.47 ip4:147.243.1.48 -all"
microsoft.com.	3600	IN	TXT		"docusign=d5a3737c-c23c-4bd0-9095-d2ff621f2840"
microsoft.com.	3600	IN	TXT		"FbUF6DbkE+Aw1/wi9xgDi8KVrIIZus5v8L6tbIQZkGrQ/rVQKJi8CjQbBtWtE64ey4NJJwj5J65PIggVYNabdQ=="
microsoft.com.	3600	IN	MX	10	microsoft-com.mail.protection.outlook.com.

Kemudian diatas merupakan data DNS records yang didapatkan untuk digunakan Microsoft.com.

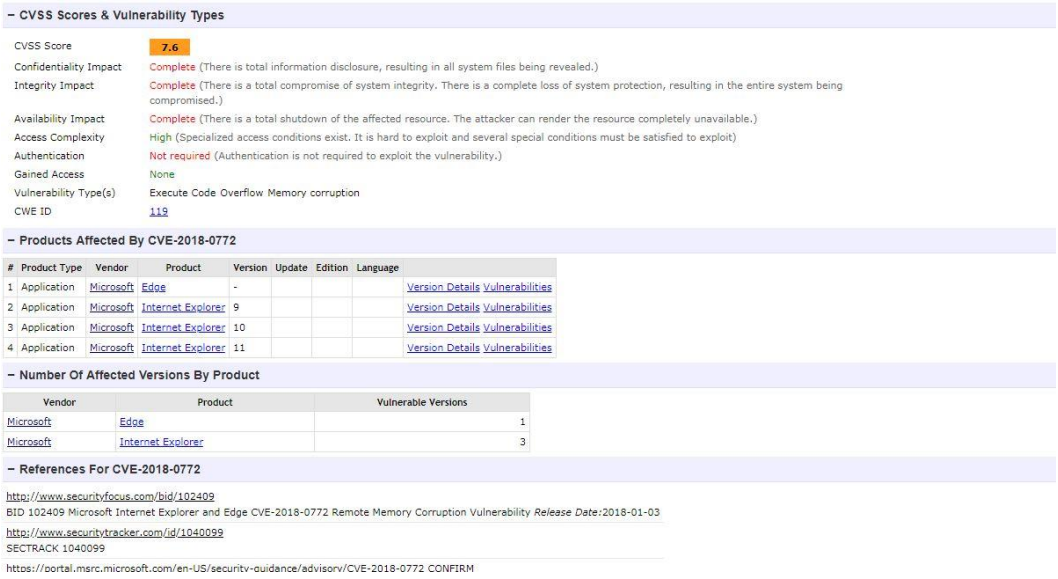
Lubang keamanan terus-menerus ditemukan di semua jenis perangkat lunak anti virus dan untuk menyambungkannya ke vendor perangkat lunak mengeluarkan tambalan - juga disebut "perbaikan" atau hanya sekadar "pembaruan keamanan" - untuk menawarkan solusi perbaikan cepat segera untuk masalah dan / atau umum peningkatan perangkat lunak.

Cacat dalam perangkat lunak Microsoft nampaknya paling populer untuk dieksploitasi, sehingga raksasa perangkat lunak Amerika Serikat mengeluarkan banyak tambalan. Tapi aplikasi desktop umum lainnya seperti Firefox, QuickTime, RealPlayer, Adobe Reader, Adobe Flash Player, dan Sun Java Runtime Environment juga perlu ditambal sering untuk memperbaiki masalah keamanan.

Pada tahun 2003, Microsoft memperkenalkan Patch Selasa untuk menyederhanakan manajemen patch. Patch Selasa adalah hari Selasa kedua setiap bulannya, saat Microsoft merilis perbaikan terbaru untuk Windows dan aplikasi perangkat lunak terkait seperti Internet Explorer, Office suite, dan Windows Media Player.

Patch Microsoft didistribusikan melalui Pembaruan Otomatis dan situs download Microsoft Update milik perusahaan.

Sayangnya, pelepasan tambalan juga berarti bahwa penjahat dunia maya dapat menganalisis kode tempel dan memanfaatkan kerentanan yang harus ditangani oleh patch tersebut. Oleh karena itu banyak eksploitasi terlihat segera setelah peluncuran sebuah patch dan istilah "Exploit Wednesday" diciptakan untuk hari setelah Patch Selasa. Penulis perangkat lunak perusak juga tahu bahwa jika mereka mulai mengeksploitasi kerentanan yang tidak diketahui Microsoft tepat setelah Patch pada hari Selasa, biasanya akan menjadi satu bulan penuh sebelum Microsoft merilis sebuah patch untuk memperbaikinya.



– CVSS Scores & Vulnerability Types

CVSS Score	7.6
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	High (Specialized access conditions exist. It is hard to exploit and several special conditions must be satisfied to exploit)
Authentication	Not required (Authentication is not required to exploit the vulnerability.)
Gained Access	None
Vulnerability Type(s)	Execute Code Overflow Memory corruption
CWE ID	119

– Products Affected By CVE-2018-0772

#	Product Type	Vendor	Product	Version	Update	Edition	Language	
1	Application	Microsoft	Edge	-				Version Details Vulnerabilities
2	Application	Microsoft	Internet Explorer	9				Version Details Vulnerabilities
3	Application	Microsoft	Internet Explorer	10				Version Details Vulnerabilities
4	Application	Microsoft	Internet Explorer	11				Version Details Vulnerabilities

– Number Of Affected Versions By Product

Vendor	Product	Vulnerable Versions
Microsoft	Edge	1
Microsoft	Internet Explorer	3

– References For CVE-2018-0772

http://www.securityfocus.com/bid/102409
BID 102409 Microsoft Internet Explorer and Edge CVE-2018-0772 Remote Memory Corruption Vulnerability *Release Date:*2018-01-03

http://www.securitytracker.com/id/1040099
SECTRACK 1040099

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0772 CONFIRM

Penjahat cyber hari ini sangat cepat dalam menciptakan kode eksploitasi. Saat Microsoft mengeluarkan tambalan, mengeksploitasi kode untuk kerentanan yang diungkapkan secara umum biasanya akan muncul sama atau hari berikutnya. Hacker bisa melakukan itu melalui reverse engineering.

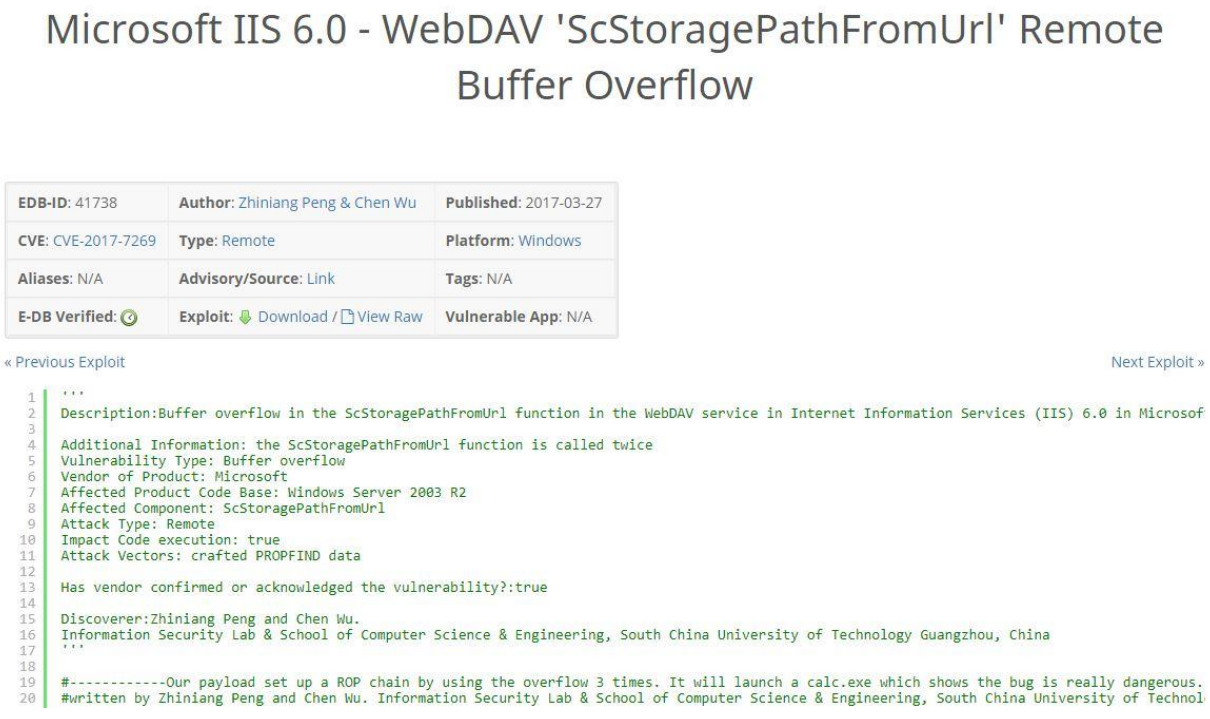
Pada bulan April 2008, sekelompok peneliti komputer mendesak Microsoft untuk mendesain ulang cara penyebarannya, setelah mereka menciptakan sebuah teknik yang secara otomatis menghasilkan kode serangan dengan membandingkan versi program yang rentan dan diperbaiki.

Serangan yang terkenal berdasarkan lubang keamanan adalah Operation Aurora, sebuah serangan malware yang ditargetkan terhadap setidaknya 30 perusahaan besar - termasuk Google dan Adobe - yang mengeksploitasi kelemahan zero-day di Internet Explorer. Eksploitasi memungkinkan malware dimuat ke komputer pengguna. Begitu dimuat, malware bisa mengendalikan komputer untuk mencuri kekayaan intelektual perusahaan.

dimuat, malware bisa mengendalikan komputer untuk mencuri kekayaan intelektual perusahaan.

Sebagai kesimpulan, dengan menggunakan alat otomatis, sebuah eksploitasi dapat dibuat dalam beberapa menit atau kurang setelah melihat patch tersebut, menurut para periset. Ini berarti secara teoritis mungkin bagi peretas untuk mulai mencoba mengeksploitasi mesin dalam waktu singkat setelah penyerang menerima patch tersebut, menempatkan lebih banyak PC yang berisiko terinfeksi perangkat lunak berbahaya.

Penyerangan



Microsoft IIS 6.0 - WebDAV 'ScStoragePathFromUrl' Remote Buffer Overflow

EDB-ID: 41738	**Author**: Zhiniang Peng & Chen Wu	**Published**: 2017-03-27
CVE: CVE-2017-7269	**Type**: Remote	**Platform**: Windows
Aliases: N/A	**Advisory/Source**: Link	**Tags**: N/A
E-DB Verified:	**Exploit**: Download / View Raw	**Vulnerable App**: N/A

« Previous Exploit Next Exploit »

```
'''
Description:Buffer overflow in the ScStoragePathFromUrl function in the WebDAV service in Internet Information Services (IIS) 6.0 in Microsof

Additional Information: the ScStoragePathFromUrl function is called twice
Vulnerability Type: Buffer overflow
Vendor of Product: Microsoft
Affected Product Code Base: Windows Server 2003 R2
Affected Component: ScStoragePathFromUrl
Attack Type: Remote
Impact Code execution: true
Attack Vectors: crafted PROPFIND data

Has vendor confirmed or acknowledged the vulnerability?:true

Discoverer:Zhiniang Peng and Chen Wu.
Information Security Lab & School of Computer Science & Engineering, South China University of Technology Guangzhou, China
'''

#------------Our payload set up a ROP chain by using the overflow 3 times. It will launch a calc.exe which shows the bug is really dangerous.
#written by Zhiniang Peng and Chen Wu. Information Security Lab & School of Computer Science & Engineering, South China University of Technol
```