

Matthew “j00ru” Jurczyk, Gynvael Coldwind
HISPASEC

CASE STUDY OF RECENT WINDOWS VULNERABILITIES

Eyjafjallajökull

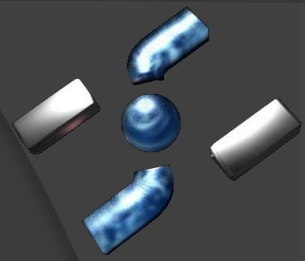
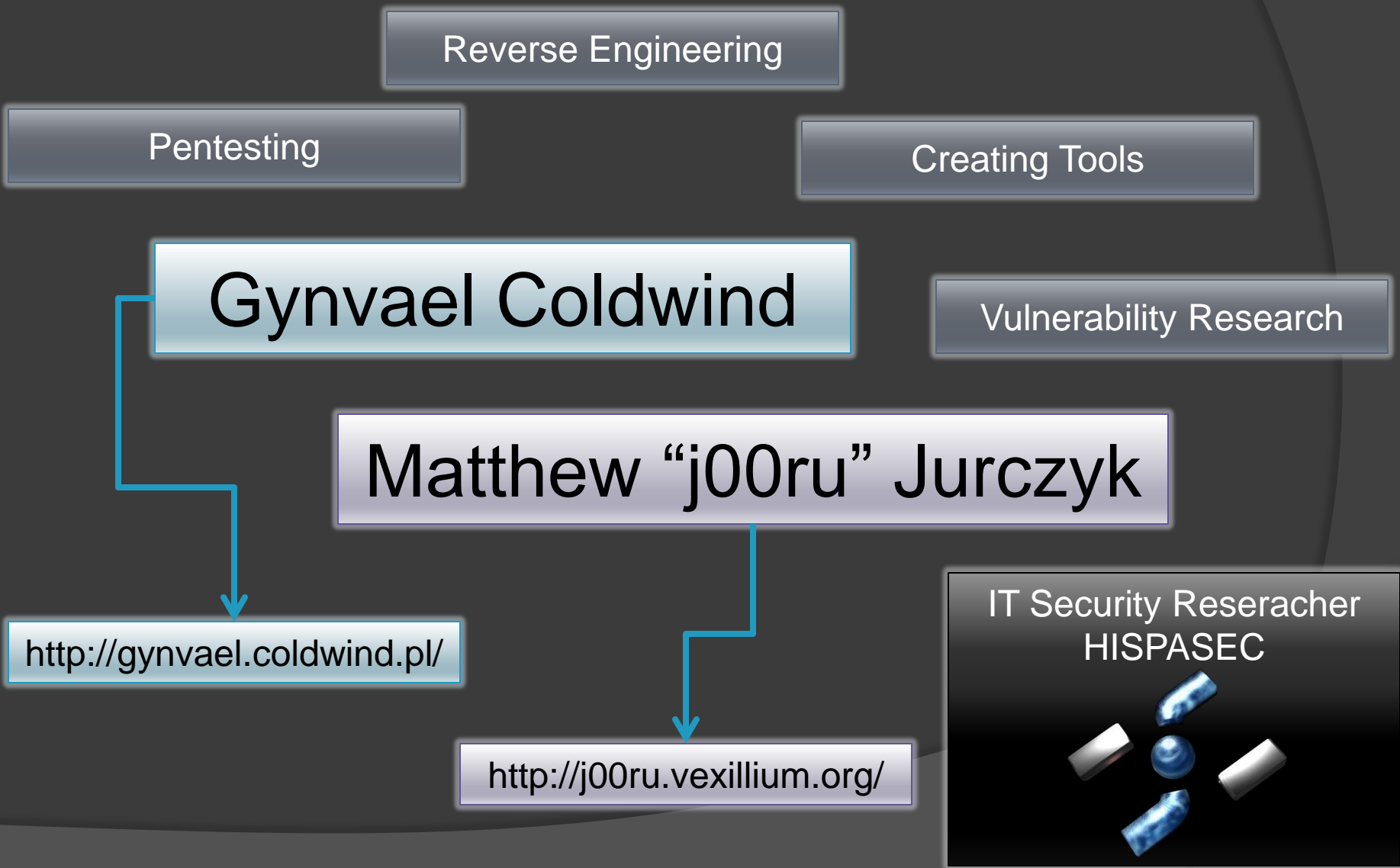


Photo by Árni Friðriksson



Me, Myself and I



Me, Myself and I



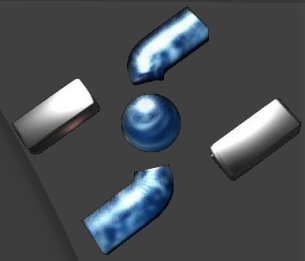
Matthew “j00ru” Jurczyk

Me, Myself and I



Gynvael Coldwind

7 vulnerabilities agenda



CSRSS Local Elevation of Privileges

Registry Link Unicode Parity Buffer Overflow DoS

Registry Link 16-bit Integer Wrap Buffer Overflow Local Elevation of Privileges

Registry Link Access Control List NULL Pointer Dereference DoS

Registry Link Race Condition DoS

Registry Link Cross-Hive Registry Information Disclosure

Registry Link Cross-Hive Local Elevation of Privileges

CSRSS Local Elevation of Privileges

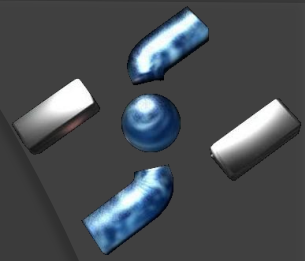
CVE-2010-0023



Affected Windows versions:

- Windows 2000 x86 SP4
- Windows XP x86 SP2 & SP3
- Windows XP x86-64 SP2
- Windows Server 2003 x86 SP2
- Windows Server 2003 x86-64 SP2
- Windows Server 2003 Itanium SP2

DEMO 1



CSRSS – what is it?

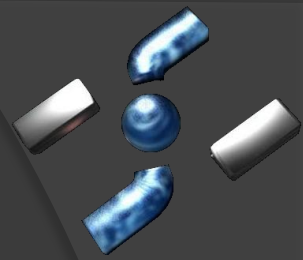


Image Name	User Name
csrss.exe	SYSTEM

Client/Server Runtime Subsystem

Csrsvr.dll

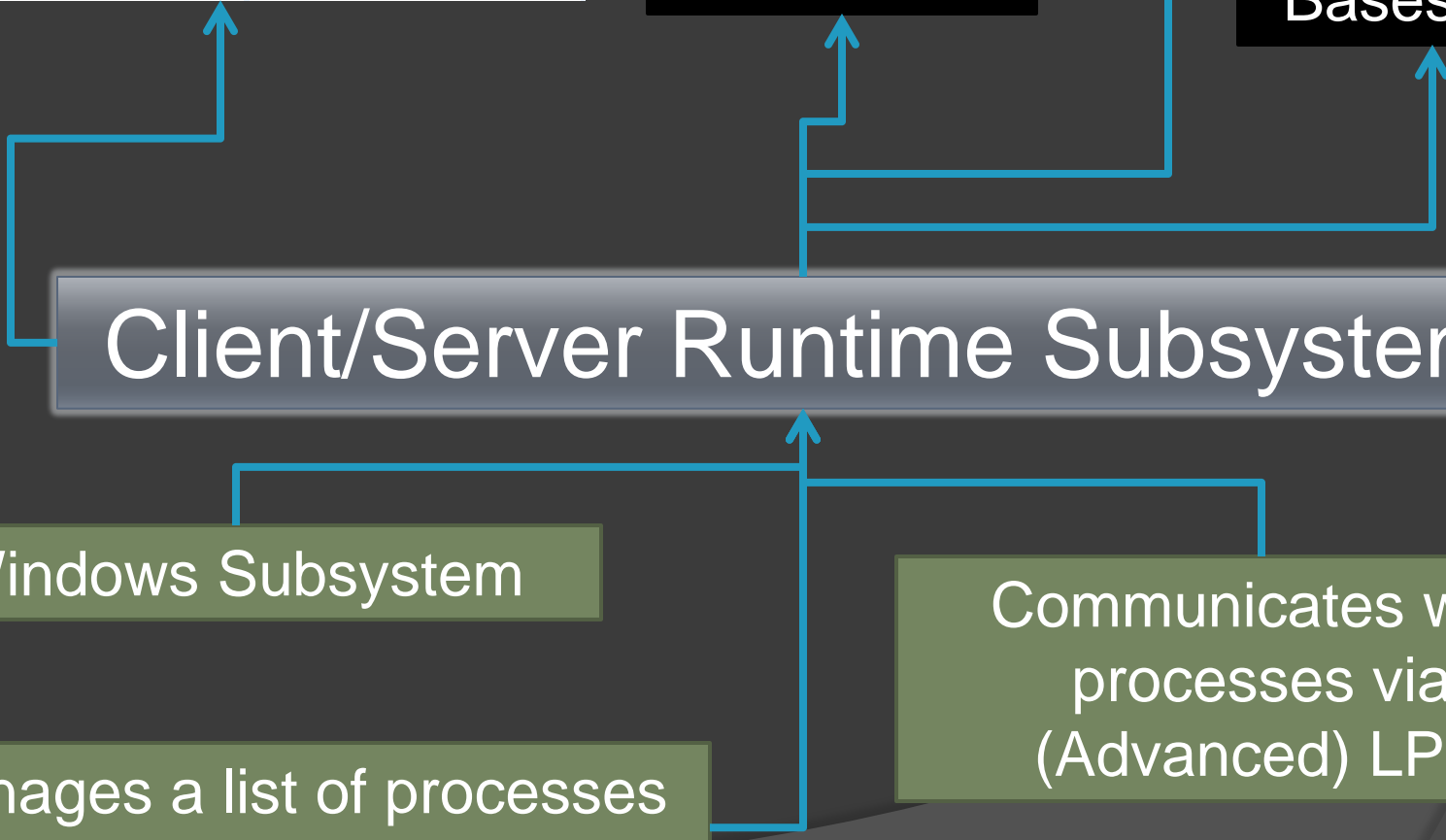
Winsrv.dll

Basesrv.dll

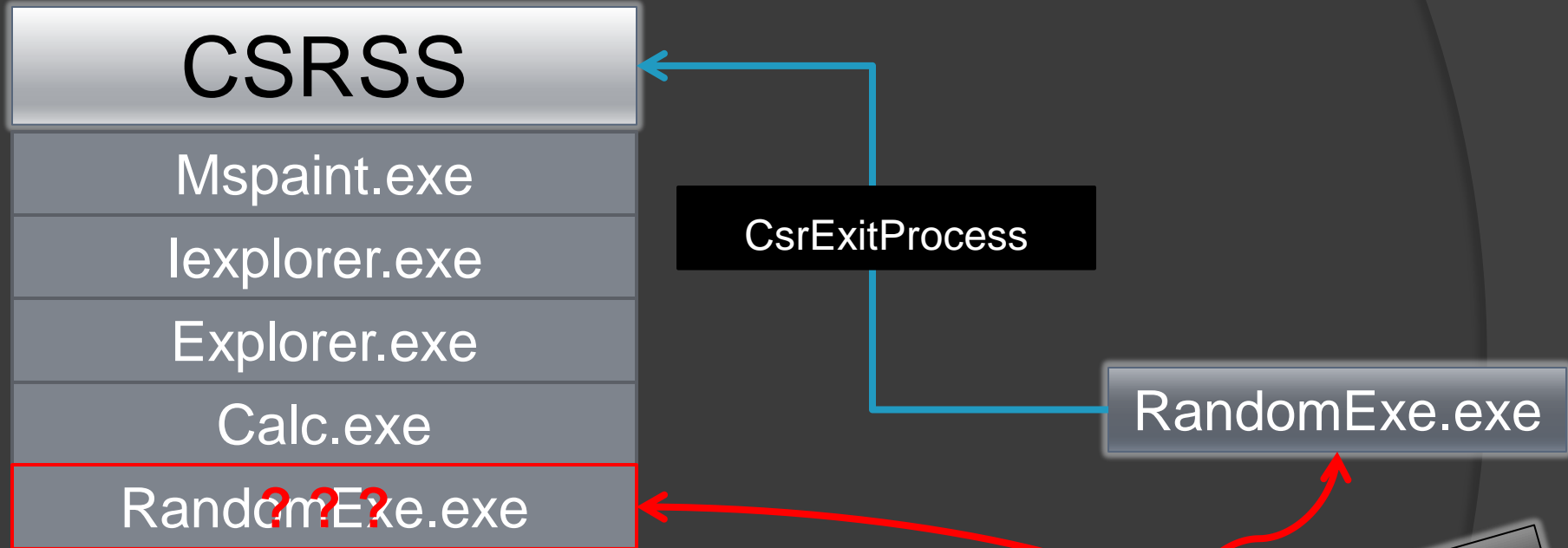
Windows Subsystem

Communicates with processes via (Advanced) LPC

Manages a list of processes
The list is used to kill them

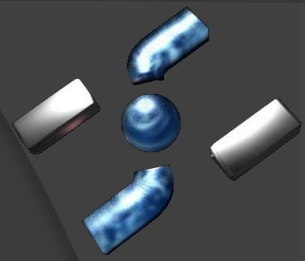


CSRSS – vulnerability?



Presenting:
The vulnerability!
☺

CSRSS – how the exploit works



Presenting... The Evil Not-Maid (but similar) Attack!



Plant exploit



Admin log in



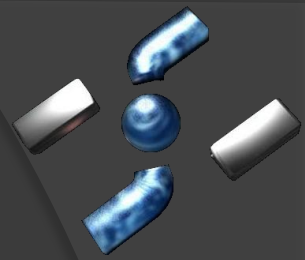
Come back



trigger

CSRSS – what does work?

Not everything from the API works when CSRSS thinks the process is dead!



Displaying windows

Sending key strokes

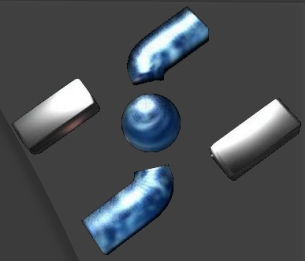
Enumerating windows

Making screenshots

Keylogging

CSRSS – how the exploit works

Immortal Exploit



1. Send the CsrExitProcess opcode

2. Log off

3. Wait for another user (admin!) to log on

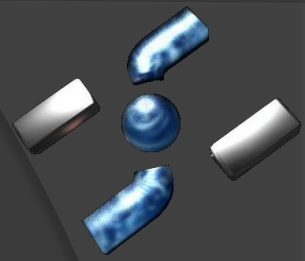
4. Take a screen shot*

5. Display the screen shot top most*

6. Run “net localgroup administrators add EvilNotMaid”*

7. Let the user log off, and relog as admin 😊

CSRSS - how the exploit works



DEMO 2 Again

Registry Link Unicode Parity Buffer Overflow DoS

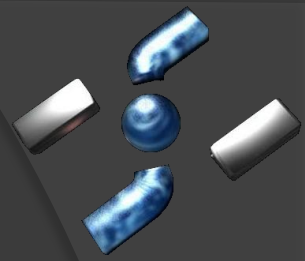
CVE-2010-0235



Affected Windows versions:

- Windows 2000 SP4
- Windows XP SP2 & SP3
- Windows Server 2003 SP2
- Windows Vista Gold

DEMO 3

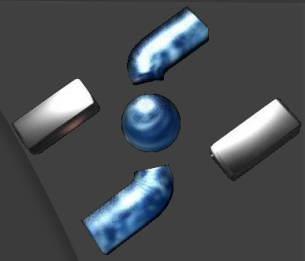


Registry – what is a Link?



No magic here 😊
Just plain simple “this key points somewhere else”

Registry – what is a Link? Technically...



REG_LINK type key

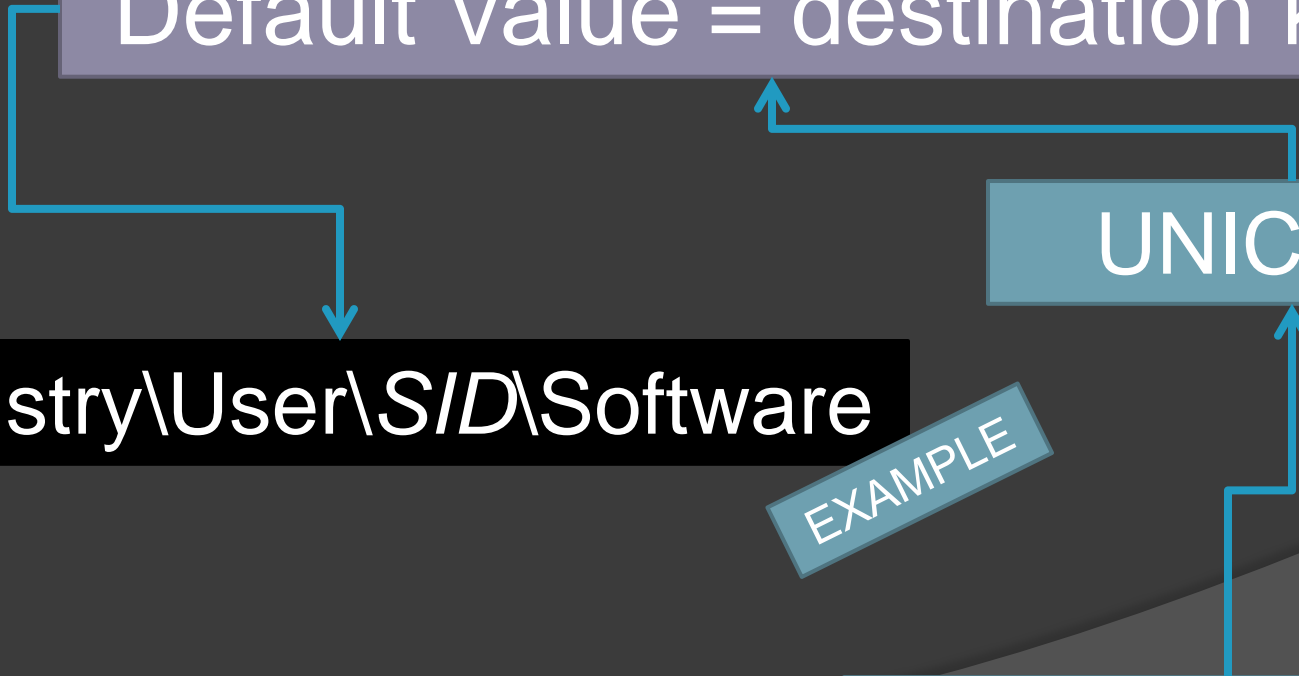
Default Value = destination key

UNICODE

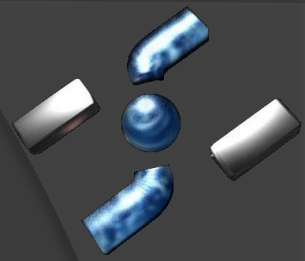
`\Registry\User\SID\Software`

EXAMPLE

2-bytes per char



Registry – How to create a link?



REGLN by Antoni Sawicki
<http://www.tenox.tc/out/#regln>

OR

`NtCreateKey` with `REG_OPTION_CREATE_LINK`
`NtSetValueKey` with `REG_LINK`

2

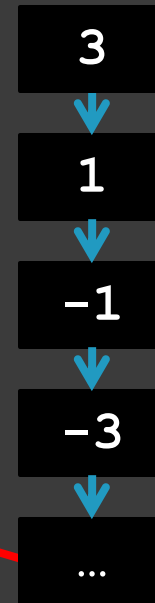
`L"SymbolicLinkValue"`

Registry – the vulnerability?

```
NtSetValueKey(  
    IN HANDLE KeyHandle,  
    IN PUNICODE_STRING ValueName,  
    IN ULONG TitleIndex OPTIONAL,  
    IN ULONG Type,  
    IN PVOID Data,  
    IN ULONG DataSize);
```

```
Count = DataSize;  
while (Count)  
{  
    [...]  
    Count -= sizeof(WCHAR);  
    [...]  
}
```

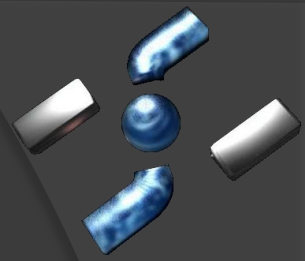
2-bytes per char



What if DataSize
is odd?
E.g. 3?

Presenting:
The vulnerability!
☺

Registry Link Unicode Parity Buffer Overflow
DoS



DEMO 4 Again

Registry Link 16-bit Integer Wrap Buffer Overflow Local Elevation of Privileges

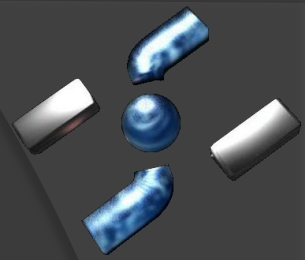
CVE-2010-0236



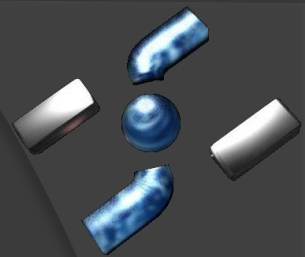
Affected Windows versions:

- Windows 2000 SP4
- Windows XP SP2 & SP3
- Windows Server 2003 SP2
- Windows Vista Gold

DEMO 5



Creating Symbolic Link Chains – what is it?



`\Registry\Machine\SymbolicLink1`



`\Registry\User\SID\SymbolicLink2`



`\Registry\Machine\SOFTWARE\SymbolicLink3`



...

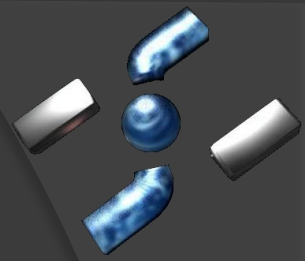
Registry Link
Chaining

Each key points to the successive
key (link) ...

... till a normal key is encountered

Chained Symbolic Link Management

CmpGetSymbolicLink function



1. Get the L"SymbolicLinkValue" value contents

2. `Length = (USHORT)ValueLength + sizeof(WCHAR);`

3. Check if `Length > 0xFFFF` ← Sanity check fail ☺

4. If `Length > Current Buffer's Length`

4.1. Reallocate the existing buffer, using `Length`

5. Copy the value data into the buffer, using `ValueLength`

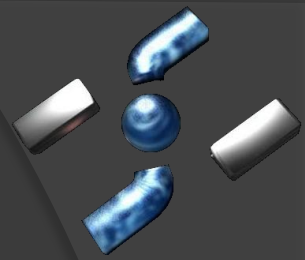
CURRENT NAME BUFFER

NEW NAME



Chained Symbolic Link Management

CmpGetSymbolicLink function



0x0000567A

0x00005678

0x12345678

```
Length = (USHORT)ValueLength + ...
```

What if
ValueLength > 0xFFFF ?

```
if (Length > CurrentLength)
```

0x0000567A

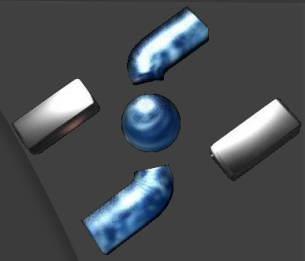
```
Buffer = Reallocate(Length);
```

```
Copy (Buffer, Data, ValueLength);
```

0x12345678

Presenting:
The vulnerability!
☺

Registry Link 16-bit Integer Wrap Buffer Overflow
Local Elevation of Privileges



DEMO 6

Again

Registry Link Access Control List NULL Pointer Dereference DoS

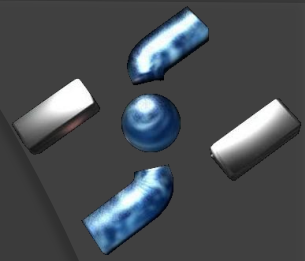
CVE-2010-0234



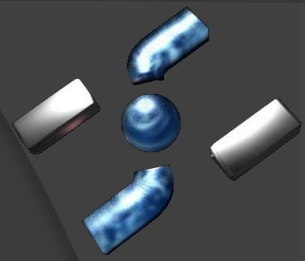
Affected Windows versions:

- Windows 2000 SP4
- Windows XP SP2 & SP3
- Windows Server 2003 SP2
- Windows Vista Gold, SP1, SP2
- Windows Server 2008 Gold, SP2

DEMO 7



Registry Symbolic Link capabilities



Transparent for **reading**:

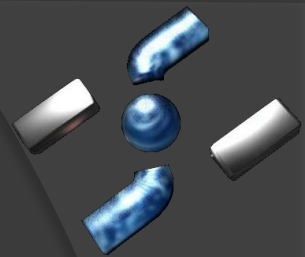
- RegQueryValue
- RegQueryMultipleValues
- RegQueryInfoKey

Transparent for **writing**:

- RegSetKeyValue
- RegSetValue
- RegCreateKey

How about security
rights?

Registry Symbolic Link – security access rights



The kernel fails to parse the symbolic link name

CompleteName parameter:

```
kd> dt nt!_UNICODE_STRING
+0x000 Length      : 0
+0x002 MaximumLength : 0
+0x004 Buffer      : (null)
```

NtOpenKey

ObOpenObjectByName

ObpLookupObjectName

CmpParseKey

CmpGetSymbolicLink

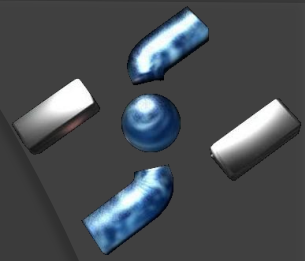
ExFreePoolWithTag(NULL);

KeBugCheckEx(0x40);

Presenting:
The vulnerability!
☺

```
A problem has been detected and windows has been shut down to prevent damage to your computer.
STOP: 0x00000001 (0x0000000C, 0x00000001, 0x00000000, 0x00000000)
If this is the first time you've seen this stop error screen,
restart your computer. If this screen appears again, follow
these steps:
Check to make sure any new hardware or software is properly installed.
If this is a new installation, ask your hardware or software manufacturer
for any windows updates you might need.
If problems continue, disable or remove any newly installed hardware
or software, disable BIOS memory options such as caching or shadowing.
If you need to use safe mode to remove or disable components, restart
your computer, press F8 to select Advanced Startup options, and then
select safe mode.
Technical information:
*** STOP: 0x00000001 (0x0000000C, 0x00000001, 0x00000000, 0x00000000)
*** g3.sys - Address F8054890 base at F8051000, DateStamp 3549194b
Beginning dump of physical memory.
Physical memory dump complete.
Contact your system administrator or technical support group for further
assistance.
```

Registry Symbolic Link – security access
rights



DEMO 8 AGAIN

Registry Link Race Condition DoS

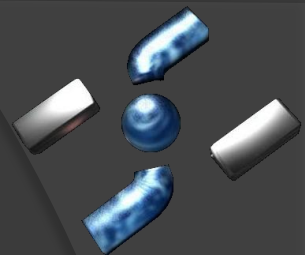
CVE-2010-0238



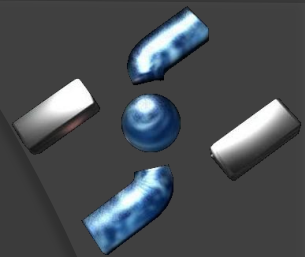
Affected Windows versions:

- Windows 2000 SP4
- Windows XP SP2 & SP3
- Windows Server 2003 SP2
- Windows Vista Gold

DEMO 9



Registry Link Race Condition DoS



Is registry access through links thread-safe?

Mmm... nope!

Fine, how do we check it?

Let's reference a link through MAANY threads! 😊

Registry Link Race Condition DoS

100 seems to be enough

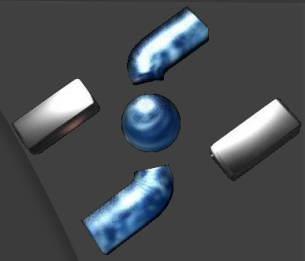
```
for( int i=0;i<NumberOfThreads;i++ )  
{  
    CreateThread(ThreadRoutine);  
}
```

```
while(1)  
{  
    RegOpenKeyEx(RegistryLink);  
}
```

The results?

You've seen it already 😊

Registry Link Race Condition DoS - details



User-mode address

`NtOpenKey (KeyHandle, Access, ObjectAttributes)`

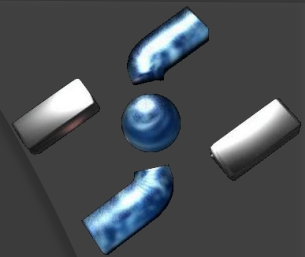
`ObOpenObjectByName (ObjectAttributes, ...`

`ObpLookupObjectName (RootDirectory~, ObjectName, ...`

On multiple references...

... the synchronization fails 😊

Registry Link Race Condition DoS - details



Just like that:

```
eax=00f8000f ebx=f40b6c68 ecx=e1dab000 edx=00000011  
esi=0052005c edi=00000000 eip=80563ed6 esp=f40b6bd0  
ebp=f40b6c28 iopl=0      nv up ei ng nz ac pe cy  
cs=0008  ss=0010  ds=0023  es=0023  fs=0030  gs=0000             efl=00010297
```

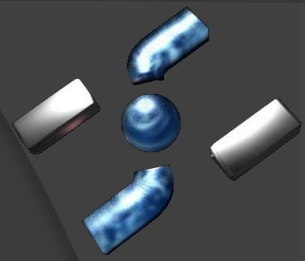
nt!ObpLookupObjectName+0x355:

```
0008:80563ed6 6683395c      cmp     word ptr [ecx],5Ch ds:0023:e1dab000=????
```

Deallocated buffer

Presenting:
The vulnerability!
☺

Registry Link Race Condition DoS



DEMO 9 AGAIN

Registry Link Cross-Hive Registry Information Disclosure

CVE-2010-0237
2 in 1



Affected Windows versions:

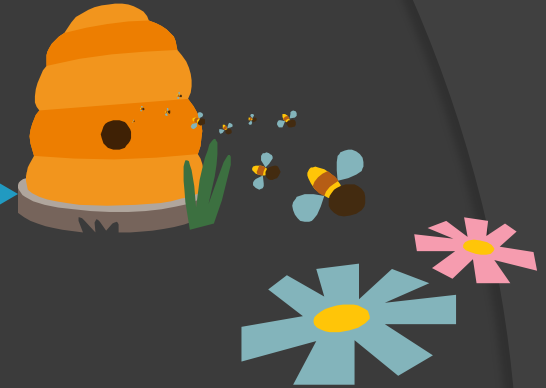
- Windows 2000 x86 SP4
- Windows XP x86 SP2 & SP3
- Windows XP x86-64 SP2

DEMO 10

Registry Hive – what is it ?

Registry split into hives

Each hive is in a separate file



Registry hive	Supporting files
HKEY_CURRENT_CONFIG	System, System.alt, System.log, System.sav
HKEY_CURRENT_USER	Ntuser.dat, Ntuser.dat.log
HKEY_LOCAL_MACHINE\SAM	Sam, Sam.log, Sam.sav
HKEY_LOCAL_MACHINE\Security	Security, Security.log, Security.sav
HKEY_LOCAL_MACHINE\Software	Software, Software.log, Software.sav
HKEY_LOCAL_MACHINE\System	System, System.alt, System.log, System.sav
HKEY_USERS\DEFAULT	Default, Default.log, Default.sav

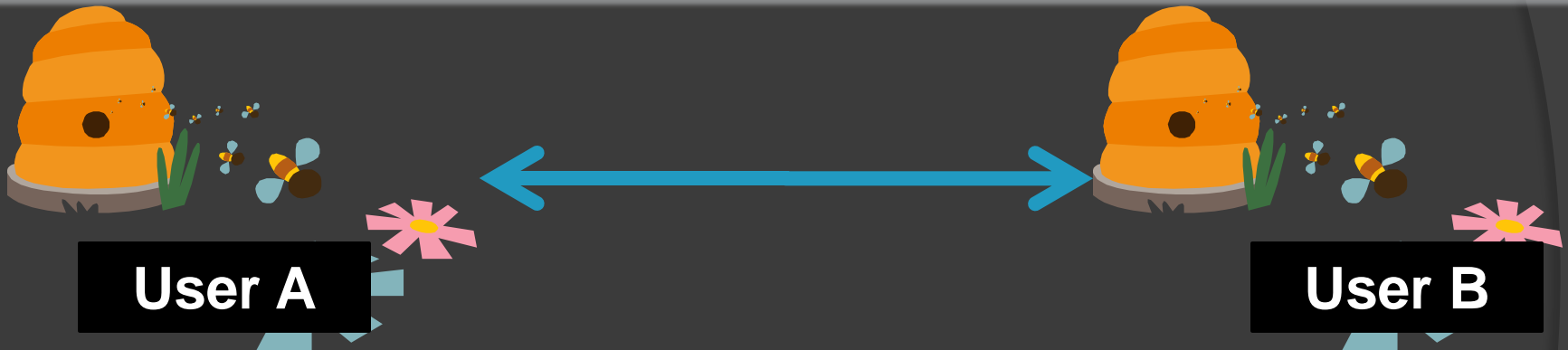
Registry Hive – links between untrusted hives

Do links between hives work ?

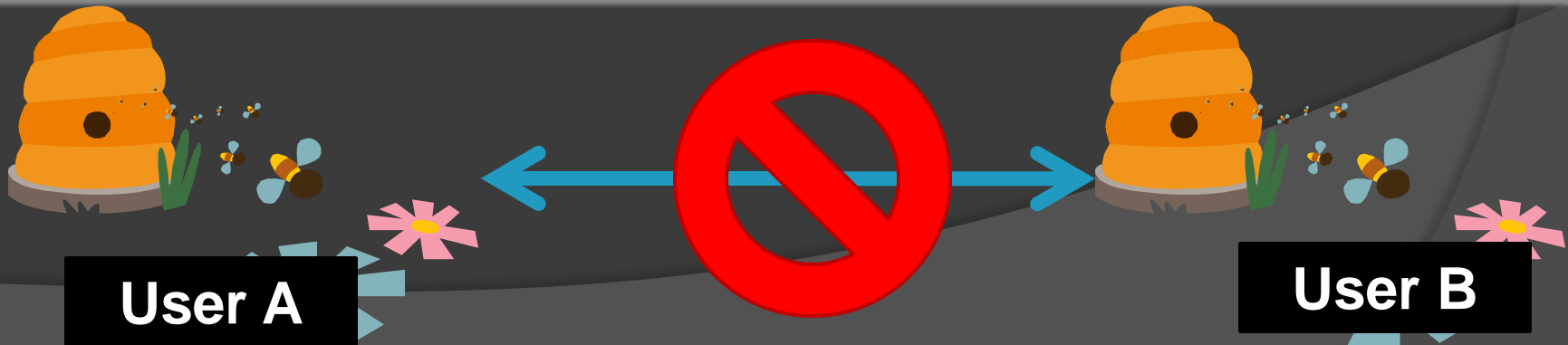
YES – in case of trusted hives

It depends in other case

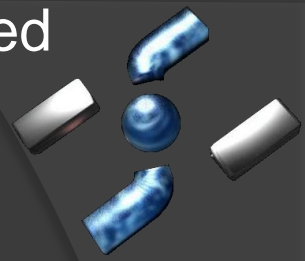
Windows 2000, XP



Vista, 7

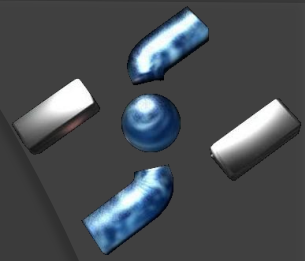


Registry – Can we write data to another hive or read protected keys there?



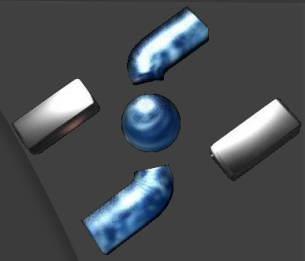
NO

Registry – Can we do the same **USING A LINK?**



NO

Registry – Do we know someone who can?



Ehm, yeah, sure...

**Any admin-level user or a process he owns
Or any SYSTEM process**



But why would they???

(... disclose the data or overwrite sth)



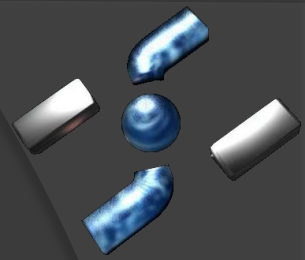
**Because we TRICK them into doing it!
(using registry links of course 😊)**

Registry – “could you read that for me sonny?”

Winlogon.exe



The attacker
(in disguise)



Registry – “could you read that for me sonny?”

Winlogon.exe

Handles the user logging in

Fetches the environment variables from the registry

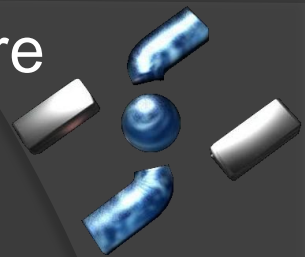
One of the things it does...

Presenting:
The vulnerability!
☺

Let's redirect this!

HKEY_CURRENT_USER\Environment\

```
15:38:00 gynvael >set
ALLUSERSPROFILE=C:\ProgramData
APPDATA=C:\Users\gynvael\AppData\Roaming
AUR32_HOME=d:\bin\avr
CommonProgramFiles=C:\Program Files (x86)\Common Files
CommonProgramFiles(x86)=C:\Program Files (x86)\Common Files
CommonProgramW6432=C:\Program Files\Common Files
COMPUTERNAME=EMERALD
```



DEMO 10
again 😊

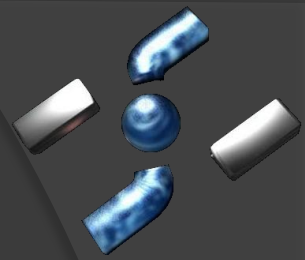
Registry Link Cross-Hive Local Elevation of Privileges

CVE-2010-0237
2 in 1



Can we use this to write something someplace?

DEMO 11



Registry Link Priv. Escal. – How?

Winlogon.exe

Handles the user logging in





Setup the paths to My Documents
Desktop, Send To, etc.

Another thing it does...

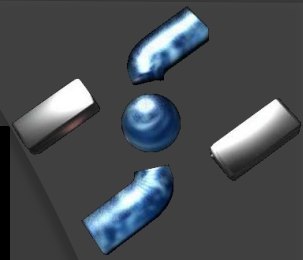
Let's redirect this!

HKEY_CURRENT_USER\Software\Microsoft\Windows\
CurrentVersion\Explorer\Shell Folders





Presenting:
The vulnerability!
☺

 Local AppData	REG_SZ	C:\Users\gynva...
 My Music	REG_SZ	C:\Users\gynva...
 My Pictures	REG_SZ	C:\Users\gynvael\Pictures
 My Video	REG_SZ	C:\Users\gynvael\Videos

Registry Link Priv. Escal. – Where do we redirect?



```
HKEY_CURRENT_USER\Software\Microsoft\Windows\
CurrentVersion\Explorer\Shell Folders
```

 Local AppData	REG_SZ	C:\Users\gynvael\AppData\Local
 My Music	REG_SZ	C:\Users\gynvael\Music
 My Pictures	REG_SZ	C:\Users\gynvael\Pictures
 My Video	REG_SZ	C:\Users\gynvael\Videos

“Run C:\Users\Attacker\Music??? It will just open the view of that folder lol”

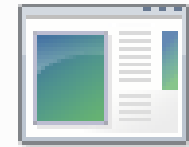
Thank you Microsoft!



Music.exe



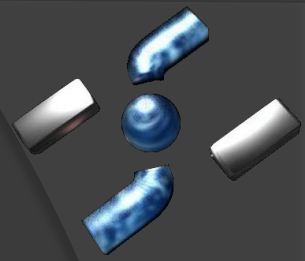
Music.bat



Music.com

```
HKEY_USERS\*AdminsSID*\Software\Microsoft\
Windows\CurrentVersion\Run
```

CVE-2010-0237
2 in 1



DEMO 11

Again

Summary & random thoughts

CSRSS Local Elevation of Privileges

Registry Monitor - Sysinternals: www.sysinternals.com

#	Time	Process	Request	Path	Result	Other
11453	7.27508938	lsass.exe:588	OpenKey	HKLM\SECURITY\Policy\SecDesc	SUCCESS	Key: 0xE1239A08
11454	7.27511035	lsass.exe:588	QueryValue	HKLM\SECURITY\Policy\SecDesc\{Default}	NOTFOUND	NDNE
11455	7.27513675	lsass.exe:588	CloseKey	HKLM\SECURITY\Policy\SecDesc	SUCCESS	Key: 0xE1239A08
11456	7.27601939	lsass.exe:588	CloseKey	HKLM\SECURITY\Policy	SUCCESS	Key: 0xE1148FB8
11457	7.56869733	svchost.exe:228	OpenKey	HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\{...}	SUCCESS	Key: 0xE1589FB8
11458	7.56861722	svchost.exe:228	QueryValue	HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\{...}	NOTFOUND	
11459	7.56863947	svchost.exe:228	QueryValue	HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\{...}	NOTFOUND	
11460	7.56867970	svchost.exe:228	CloseKey	HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\{...}	SUCCESS	Key: 0xE1589FB8
11461	7.56873490	svchost.exe:228	CreateKey	HKLM\SYSTEM\ControlSet002\Services\Tcpip\Linkage\Bind	SUCCESS	Key: 0xE1589FB8
11462	7.56875530	svchost.exe:228	QueryValue	HKLM\SYSTEM\ControlSet002\Services\Tcpip\Linkage\Bind	NOTFOUND	
11463	7.56877948	svchost.exe:228	CloseKey	HKLM\SYSTEM\ControlSet002\Services\Tcpip\Linkage\Bind	SUCCESS	Key: 0xE1589FB8
11464	8.58402569	svchost.exe:228	OpenKey	HKLM\SYSTEM\ControlSet002\Services\Tcpip\Linkage\Bind	SUCCESS	Key: 0xE1589FB8
11465	8.58405286	svchost.exe:228	QueryValue	HKLM\SYSTEM\ControlSet002\Services\Tcpip\Linkage\Bind	NOTFOUND	
11466	8.58407240	svchost.exe:228	OpenKey	HKLM\SYSTEM\ControlSet002\Services\Tcpip\Linkage\Bind	NOTFOUND	
11467	8.58410582	svchost.exe:228	CloseKey	HKLM\SYSTEM\ControlSet002\Services\Tcpip\Linkage\Bind	SUCCESS	Key: 0xE1589FB8
11468	8.58415875	svchost.exe:228	CloseKey	HKLM\SYSTEM\ControlSet002\Services\Tcpip\Linkage\Bind	SUCCESS	Key: 0xE1589FB8
11469	8.58417916	svchost.exe:228	CloseKey	HKLM\SYSTEM\ControlSet002\Services\Tcpip\Linkage\Bind	NOTFOUND	
11470	8.58420307	svchost.exe:228	CloseKey	HKLM\SYSTEM\ControlSet002\Services\Tcpip\Linkage\Bind	SUCCESS	Key: 0xE1589FB8
11471	8.60657617	OUTLOOK.EXE	OpenKey	HKLM\SYSTEM\ControlSet002\Services\Tcpip\Linkage\Bind	BUFDVRFLOW	
11472	8.60663872	OUTLOOK.EXE	QueryValue	HKLM\SYSTEM\ControlSet002\Services\Tcpip\Linkage\Bind	BUFDVRFLOW	
11473	8.60668959	OUTLOOK.EXE	QueryValue	HKLM\SYSTEM\ControlSet002\Services\Tcpip\Linkage\Bind	SUCCESS	"\Device\{BA820BB...}
11474	8.60798982	OUTLOOK.EXE	QueryValue	HKLM\SYSTEM\ControlSet002\Services\Tcpip\Linkage\Bind	BUFDVRFLOW	
11475	8.608002843	OUTLOOK.EXE	QueryValue	HKLM\SYSTEM\ControlSet002\Services\Tcpip\Linkage\Bind	BUFDVRFLOW	
11476	8.60807747	OUTLOOK.EXE	QueryValue	HKLM\SYSTEM\ControlSet002\Services\Tcpip\Linkage\Bind	SUCCESS	"\Device\{BA820BB...}
11477	8.61006360	OUTLOOK.EXE	OpenKey	HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\{...}	SUCCESS	Key: 0xE1589FB8
11478	8.61009992	OUTLOOK.EXE	QueryValue	HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\{...}	SUCCESS	0x1
11479	8.61013548	OUTLOOK.EXE	QueryValue	HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\{...}	SUCCESS	0x3E794ABD

Registry Link Cross-Hive Registry Information Disclosure
Registry Link Cross-Hive Local Elevation of Privileges

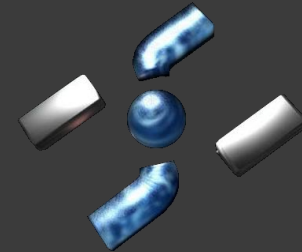
Contact



Matthew "j00ru" Jurczyk
<http://j00ru.vexillium.org/>
[mailto: j00ru@vexillium.org](mailto:j00ru@vexillium.org)



Gynvael Coldwind
<http://gynvael.coldwind.pl/>
[mailto: gynvael@coldwind.pl](mailto:gynvael@coldwind.pl)



HISPASEC
<http://hispasec.com/>
<http://virustotal.com/>