Anti-Virus Software 0Day Party

MJ0011

th_decoder@126.com

2010-12-06

Agenda

- Disclose AhnLab 0day
- Disclose NProtect 0day
- Disclose ViRotbot 0day
- Disclose ALYAC 0day
- How to prevent kernel 0day

Ahnlab V3 Internet Security Kernel 0Day

AhnRec2k.sys is possible to do local privilege escalation through ring0 code execution (<= 1.2.03 , found in 2010-8-23), which affects AhnLab V3 Internet Security.

AhnRec2k.sys does not create any symbolic link,but it also can be opened its device: \Device\AhnRec by using NtCreateFile. Attacker can send ring3 shellcode address pointer to AhnRec2k.sys , which will directly execution shellcode under the ring0 privilege

Ahnlab has tried to fix this vulnerability at 2010-10-11, use the new AhnRec2k.sys checked whether address pointer is less than MmUserHighestAddress

2010-12-06

Ahnlab V3 Internet Security Kernel 0Day

IT ALSO CAN BE EXPLOITED!

My exploit steps:

search IoStartPacket-> call dword ptr[eax+30]

eax = filesyste driver's device object

eax+30=device_object->stacksize , always <=20

Allocate vm on 0x0 , copy shellcode jump instruction to virtual address 0x20

Send call pointer IoStartPacket->call dword[eax+30] to AhnRec2k.sys

Demo: AhnRec2k.sys local privilege escalation

NProtect Kernel Mode 0Day

TkRgAc2k.sys local privilege escalation through ring0 code execution (<= 2010.5.11.1 , found in 2010-9-7), which affects NProtect AntiVirus 2007.

A "0 pointer kernel object" vulnerability , which is a type of local kernel mode vulnerability has not been publicly.

For example , KeSetEvent to a KEVENT object pointer which TkRgAc2k.sys used has been initialized to address 0x0.

Attacker can allocate a fake KEVENT structure at address 0x0 and overwrite arbitrary address with

KEvent->WaitThreadList->KThread->WaitListEntry's removing list entry.

NProtect Kernel Mode 0Day

TkAcRg2k.sys create FileObject->FsContext for each process to open the device, and save key/key value /virus name /event object in FsContext.

TkAcRg2k.sys monitors system registry access operation with CmRegistryCallback. If a registry operation is intercepted which matches the rules, regardless of whether event handle has not been set, TKAcRg2k.sys informs this event to ring3 with KeSetEvent(NULL,0).

NProtect Kernel Mode 0Day

some io control codes

0x22140C:IOCTL_GET_MONITOR_KEY_VALUE_NAME_MD5
Accpcts registry monitor key value name MD5
0x221448:IOCTL_GET_MONITOR_KEY_NAME :
Accpcts Registry monitor key name
0x221444:IOCTL_CLIENT_ENBALE_CONTROL
Registry key monitor client enable/disable
0x221410:IOCTL_GET_ALERT_VIRUS_NAME
Accpcts virus name that matchs the key value name MD5
0x220c54:IOCTL_ALLOCATE_SHARE_MEMORY
Create share memory for receive virus notification
0x220c5c:IOCTL_GET_NOTIFICATION_EVENT_HANDLE
Accpcts event handle for send virus notification

NProtect Kernel Mode 0Day

My exploit steps:

1. Allocate and fill a fake KEVENT structure at address 0x0, which will overwrite xHalQuerySystemInformation address when KeSetEvent is called with this fake KEVENT.

2. Fill registry monitor key value name MD5\registry monitor key name\virus name, create shared memory with driver.

3. Temper with current process 's PEB->ProcessParameters->ImagePathName to "iexplore.exe" , because TkAcRg2k.sys will check if MSIE accesses monitored registry key.

4. Access monitored registry key.

5. Call NtQueryIntervalProfile to tigger shellcode.

Demo: TkAcRg2k.sys local privilege escalation.

2010-12-06

NProtect Kernel 0Day

TkFsAv2k.sys local kernel D.O.S vulnerability (<= 2010.4.9.1 ,found in 2010-9-9) affects NProtect AntiVirus 2007.

This is an integer overflow vulnerability. TkFsAv2k.sys will allocate a memory buffer which length = specified length + 12 bytes , then copy the specified length of memory from irp's SystemBuffer to the memory buffer.

An Attacker can specify the length to 0xffffffff. There will only 0xffffffff+12 = 11 bytes buffer size will be allocated , and will cause a system crash.

Demo: TkFsAv2k.sys Local D.O.S

2010-12-06

ViRobot Desktop & Server 0Day

VRsecos.sys local privilege escalation through ring0 code execution (<= 2008.8.1.1 , found in 2010-8-22) affects ViRobot Desktop 5.5 and ViRobot Server 3.5

VRsecos.sys copy memory from irp 's system buffer to driver's data area by "strcpy" function. It can be overwrite critical kernel object memory in VRsecos.sys 's data area

This is only a string copy to data area but not thread stack , so there will not be any gs cookie check.

ViRobot Desktop & Server 0Day

My Exploit Method:

overwrite NPAGED_LOOKASIDE_LIST in VRsecos.sys 's data area.

Steps:

1. Fill mutant object which will be overwrited: mutant owner thread, mutant list entry, SignalState.

2. Fill NPAGED_LOOKASIDE_LIST which will be overwrited: AllocateRoutine.

3. Tigger a npaged_lookaside_list allocation.

Demo: VRsecos.sys local privilege escalation

ViRobot Desktop & Server 0Day

VRFWNTD5.sys local kernel D.O.S vulnerability (<= 2009.3.18.44 ,found in 2010-8-22) affects ViRobot Desktop & Server

This is a typical string overflow vulnerability.

VRFWNTD5.sys uses the function "sprintf" to copy memory from irp 's system buffer to kernel stack, and gs cookie check will cause system crash when uses long input data length.

Demo: TkFsAv2k.sys Local D.O.S

2010-12-06

ALYac Kernel Mode 0Day

AYDrvNT.sys local privilege escalation through ring0 code execution (<= 5.0.1.2 , found in 2010-9-7) affects ALYac AntiVirus 1.5.

AYDrvNT.sys accepts a RING3 address pointer and uses it to overwrite any system service function address.

An attacker can overwrite a system service which is not commonly used, trigger shellcode excution by calling this function.

Demo: AYDrvNT.sys local privilege escalation

2010-12-06

How to prevent kernel 0Day

Don't provide risky kernel mode interface. Do caller check strictly.

Be attention to buffer checked. Use correctly ProbeForRead/ProbeForWrite

Be attention to the length of buffer. Prevent to use buffer with the length=0 , or address pointer= 0.

Use kernel verifier and FUZZ tools.