



## ISA 2004 Beta 2 – Vulnerability Report

Case nr.: SRQ040708600628

MS Research number: MSRC5366lw

Discovered by Dennis Rand  
advisory@cirt.dk  
<http://www.cirt.dk>

## Table of contents

<b>INTRODUCTION .....</b>	<b>3</b>
<b>TIMELINE OF PUBLIC DISCLOSURE .....</b>	<b>3</b>
<b>CONTACT INFORMATION .....</b>	<b>3</b>
<b>PROBLEM.....</b>	<b>4</b>
<b>TECHNICAL DETAILS .....</b>	<b>5</b>
EVENT VIEWER INFO.....	5
<b>FILE INFORMATION .....</b>	<b>6</b>
<b>IMPACT.....</b>	<b>7</b>
<b>DISCLAIMER .....</b>	<b>9</b>

## Introduction

CIRT.DK has recently discovered an HEAP based overflow vulnerability within the ISA 2004 beta 2 servers.

Normally Beta versions are not targets for advisories, but the version was close to be put out as release in the final version, so it was accepted by Microsoft.

## Timeline of public disclosure

- Vendor contacted: 07-07-2004
  - securitycu@css.one.microsoft.com (att.: Cherlene)
  - ID: CST166415075ID
- Vendor contacted again: 08-07-2004
  - ncs@microsoft.com (att.: Lars Madsen)
  - Case ID: SRQ040708600628
- Vendor response 10-07-2004
  - ID: MSRC5366 (secure@microsoft.com)
  - Problem fixed 16-07-2004
- CERT Contacted: 07-07-2004
  - VU#656416 09-07-2004
- Public release: 25-11-2004

Should there be any problems making a fix available for this issue within the given time frame, PROTEGO A/S will move the public disclosure until Microsoft have made a patch for this issue.

## Contact information

The following vulnerability were discovered by Dennis Rand at CIRT.DK  
Questions regarding this issue, should be directed to:

Dennis Rand  
advisory@cirt.dk

## Explanation

ISA Server 2004 is Microsoft's next-generation application-layer firewall, virtual private network, and Web cache solution, delivering new levels of security, simplified management, and performance.

## Problem

The ISA 2004 server does not perform proper bounds check on requests passed to the application. This results in a heap overflow condition, when a large specially crafted request is sent to a web-server through port 80.

This problem allows attackers to cause the ISA 2004 Beta 2 to execute arbitrary code, with the rights of the service running.

As a default setting on the ISA 2004 Beta 2 server the "Request headers length" are set to 32768 bytes. Further down the configuration under URL Protection, the settings are default "Maximum URL length: 10240" and "Maximum query length: 10240". The problem exists if a request is in between these two values 32768 and the sum of URL length, and query length, 20480 bytes.

## Technical details

The installation file of ISA 2004, Beta:           ISA2K4B2EN.EXE  
Version of installation package:                 5.00.2920.0000

The Server is an Windows 2000 with all the latest patches applied.

The issue can be triggered by requesting:  
[http://\[hostname\]/\[VeryLongRequest\]](http://[hostname]/[VeryLongRequest]) on a server protected by the ISA server, while the ISA server is in Live monitoring mode.

## Event Viewer info

Event Type:	Error
Event Source:	Microsoft Firewall
Event Category:	None
Event ID:	14057
Description:	The Firewall service stopped because an application filter module C:\Program Files\Microsoft ISA Server\w3filter.dll generated an exception code C0000005 in address 10012B1C when function CompleteAsyncIO was called. To resolve this error, remove recently installed application

Event Type:	Error
Event Source:	Microsoft ISA Server
Event Category:	None
Event ID:	1000
Description:	Faulting application wpsrv.exe, version 4.0.1872.0, stamp 3fb2f88a, faulting module w3filter.dll, version 4.0.1872.0, stamp 3fb2f848, debug? 0, fault address 0x00012b1c.

## File information

This is the information regarding the files mentioned in the event viewer.

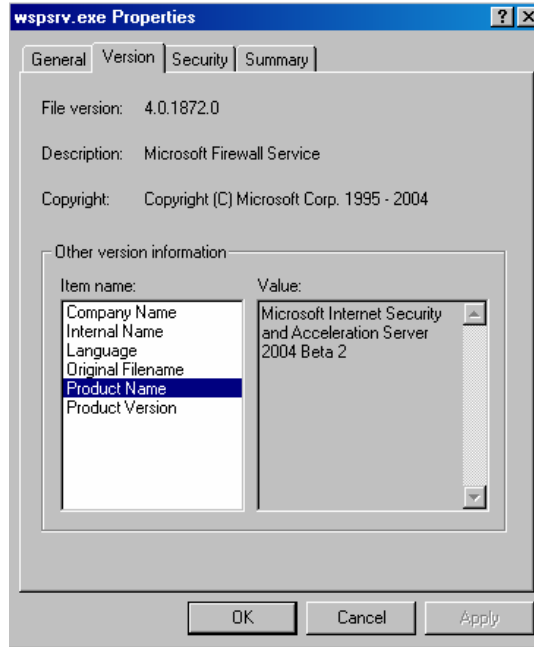


Figure 1 – WSPSRV.EXE

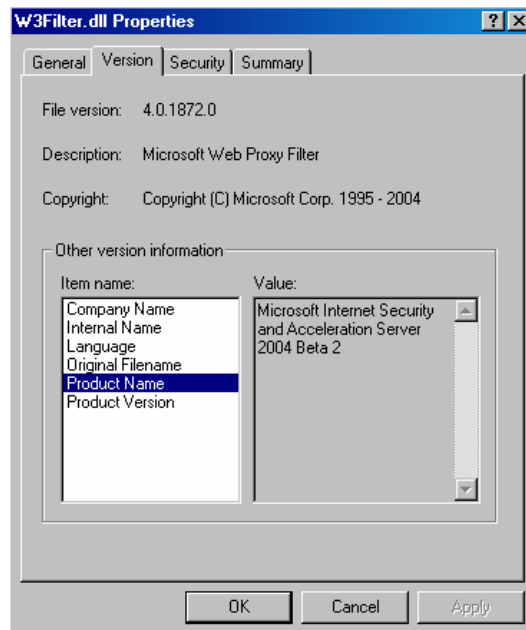
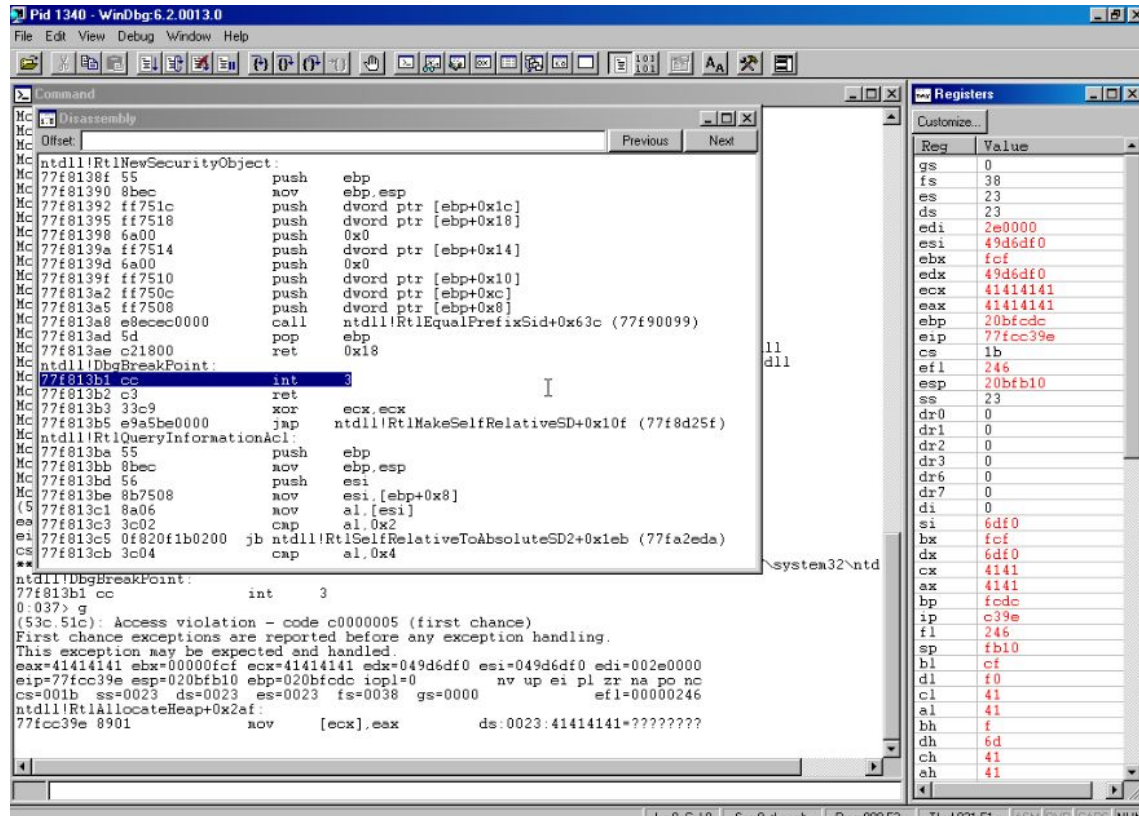


Figure 2 - W3Filter.dll

## Impact

A request like the above will overrun HEAP and overwrite the registers EAX, ECX and EDX, which leads to a service stop and of possible remote code execution.

This allows attackers to cause the ISA 2004 Beta 2 to execute arbitrary code, with the rights of the service running.



The screenshot shows the MS Debugger interface with the following assembly code in the Command window:

```
ntdll!RtlNewSecurityObject
77f8138f 55      push    ebp
77f81390 8bec    mov     ebp,esp
77f81392 ff751c  push   dword ptr [ebp+0x1c]
77f81395 ff7518  push   dword ptr [ebp+0x18]
77f81398 6a00    push   0x0
77f8139a ff7514  push   dword ptr [ebp+0x14]
77f8139d 6a00    push   0x0
77f8139f ff7510  push   dword ptr [ebp+0x10]
77f813a2 ff750c  push   dword ptr [ebp+0xc]
77f813a5 ff7508  push   dword ptr [ebp+0x8]
77f813a8 e8eccc0000 call   ntdll!RtlEqualPrefixSid+0x63c (77f90099)
77f813ad 5d      pop     ebp
77f813ae c21800  ret    0x18
ntdll!DbgBreakPoint:
77f813b1 cc      int     3
77f813b2 c3      ret
77f813b3 33c9    xor     ecx,ecx
77f813b5 e9a5be0000 jmp     ntdll!RtlMakeSelfRelativeSD+0x10f (77f8d25f)
ntdll!RtlQueryInformationAcl
77f813ba 55      push    ebp
77f813bb 8bec    mov     ebp,esp
77f813bd 56      push   esi
77f813be 8b7508  mov     esi,[ebp+0x8]
(5) 77f813c1 8a06    mov     al,[esi]
ea 77f813c3 3c02    cmp     al,0x2
e1 77f813c5 0f820f1b0200 jb     ntdll!RtlSelfRelativeToAbsoluteSD2+0x1eb (77fa2eda)
cs 77f813cb 3c04    cmp     al,0x4
ntdll!DbgBreakPoint:
77f813b1 cc      int     3
0:037> g
(53c 51c): Access violation - code c0000005 (first chance)
First chance exceptions are reported before any exception handling.
This exception may be expected and handled.
eax=41414141 ebx=000000cf ecx=41414141 edx=049d6df0 esi=049d6df0 edi=002e0000
eip=77fcc39e esp=020bfb10 ebp=020bfcdc iopl=0         nv up ei pl zr na po nc
cs=001b  ss=0023  ds=0023  es=0023  fs=0038  gs=0000             efl=00000246
ntdll!RtlAllocateHeap+0x2af:
77fcc39e 8901    mov     [ecx],eax          ds:0023:41414141+????????
```

The Registers window shows the following values:

Reg	Value
gs	0
fs	38
es	23
ds	23
edi	2e0000
esi	49d6df0
ebx	cf
edx	49d6df0
ecx	41414141
eax	41414141
ebp	20bfcdc
eip	77fcc39e
cs	1b
efl	246
esp	20bfb10
ss	23
dr0	0
dr1	0
dr2	0
dr3	0
dr6	0
dr7	0
di	0
si	6df0
bx	cf
dx	6df0
cx	4141
ax	4141
bp	fcdc
ip	c39e
fl	246
sp	fb10
bl	cf
dl	f0
cl	41
al	41
bh	f
dh	6d
ch	41
ah	41

Figure 3 – Output from MS Debugger

Figure 3 – Output from MS Debugger– Shows that the following registers have been overwritten with the value 41414141 that are the Hex value for “AAAA”

## Corrective actions

Update to latest version of the ISA 2004 server  
<http://www.microsoft.com/ISAServer/>

There is a workaround, if the configuration is changed from the default settings:

<b>Request headers length</b>	<b>32768</b>	<b>bytes</b>
<b>Maximum URL length</b>	<b>10240</b>	<b>bytes</b>
<b>Maximum query length</b>	<b>10240</b>	<b>bytes</b>

To the following:

<b>Request headers length</b>	<b>32768</b>	<b>bytes</b>
<b>Maximum URL length</b>	<b>16384</b>	<b>bytes</b>
<b>Maximum query length</b>	<b>16384</b>	<b>bytes</b>

This configuration ensures that there are no lost bytes in between "Request headers length" and the sum of "URL length" and "Query length".



## Disclaimer

The information within this document may change without notice. Use of this information constitutes acceptance for use in an "AS IS" condition.

There are NO warranties with regard to this information.

In no event shall I be liable for any consequences or damages, including direct, indirect, incidental, consequential, loss of business profits or special damages, arising out of or in connection with the use or spread of this information.

Any use of this information lies within the user's responsibility. All registered and unregistered trademarks represented in this document are the sole property of their respective owners.