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

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 responce 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] 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 wspsrv.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.

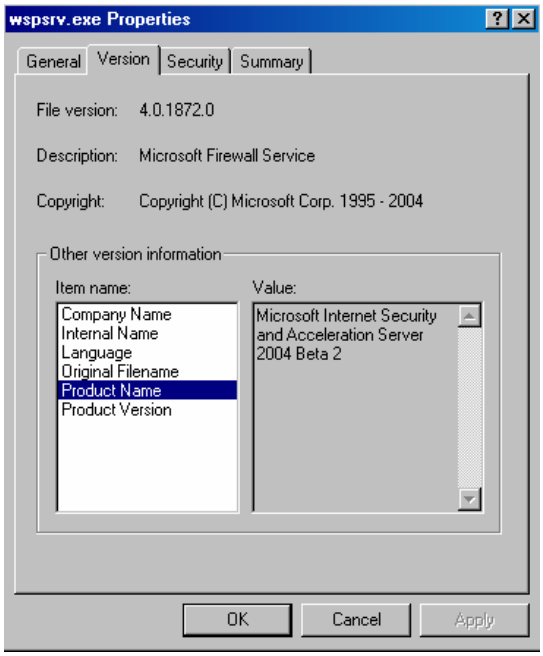

Figure 1 – WSPSRV.EXE

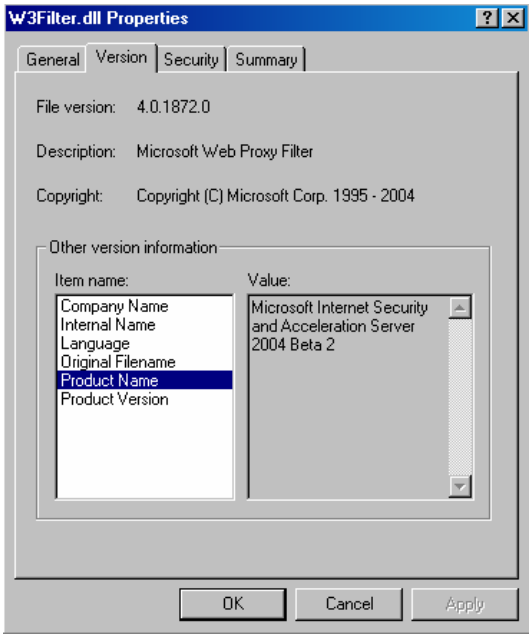

Figure 2 - W3Filter.dll

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.

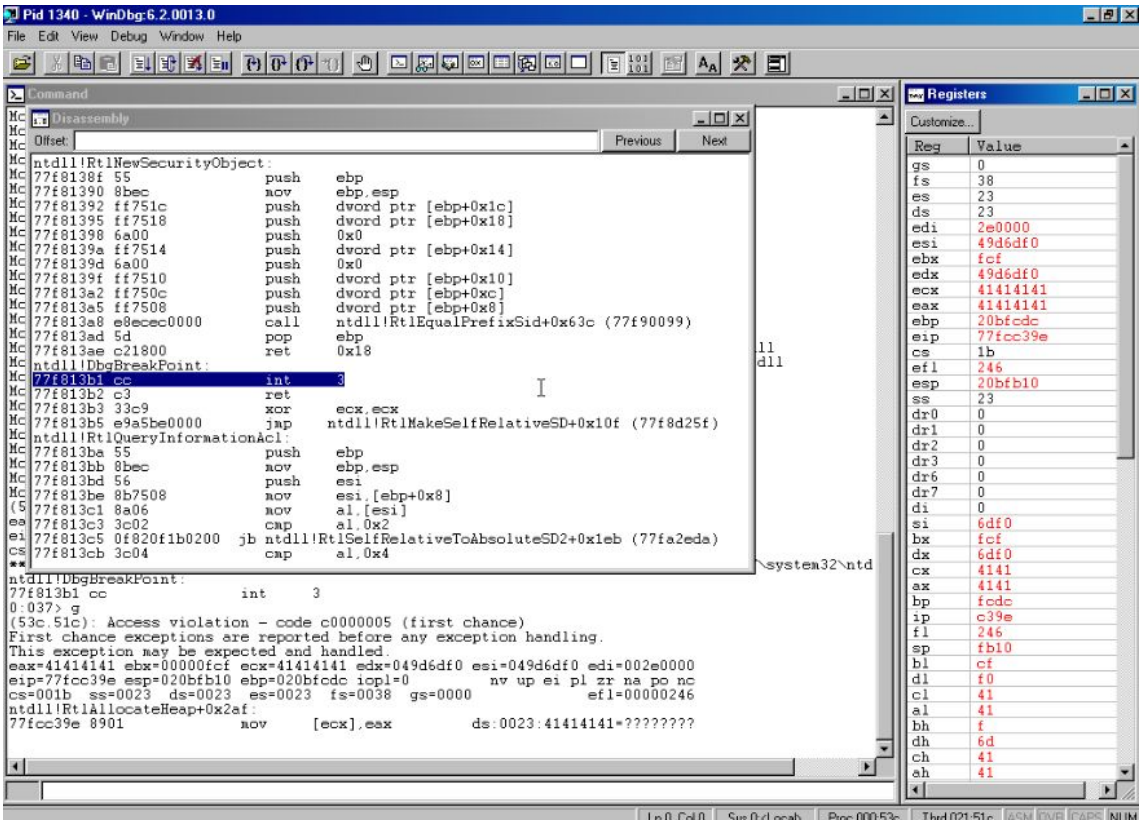

Figure 3 – Output from MS Debugger

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:

Request headers length	**32768**	**bytes**
Maximum URL length	**10240**	**bytes**
Maximum query length	**10240**	**bytes**

To the following:

Request headers length	**32768**	**bytes**
Maximum URL length	**16384**	**bytes**
Maximum query length	**16384**	**bytes**

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

Disclaimer