

# [NEWS] Trend Micro ServerProtect eng50.dll Stack Overflow Vulnerabilities

---

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2007-02/msg00071.html>

---

- *From:* SecuriTeam <[support@xxxxxxxxxxxxxx](mailto:support@xxxxxxxxxxxxxx)>
  - *Date:* 21 Feb 2007 19:10:33 +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 ServerProtect eng50.dll Stack Overflow Vulnerabilities

---

## SUMMARY

"

<<http://www.trendmicro.com/en/products/file-server/sp/evaluate/overview.htm>> ServerProtect provides comprehensive antivirus scanning for servers, detecting and removing viruses from files and compressed files in real time"

These vulnerabilities allow attackers to execute arbitrary code on vulnerable installations of Trend Micro ServerProtect. Authentication is not required to exploit these vulnerabilities.

## DETAILS

Vulnerable Systems:

- \* ServerProtect for Windows 5.58
- \* ServerProtect for EMC 5.58
- \* ServerProtect for Network Appliance Filer 5.61
- \* ServerProtect for Network Appliance Filer 5.62

The specific flaws exist within the StCommon.dll library and are reachable remotely through a DCE/RPC endpoint on TCP port 5168 bound to by the

## [NEWS] Trend Micro ServerProtect eng50.dll Stack Overflow Vulnerabilities

service SpntSvc.exe. The RPC endpoint is exposed from TmRpcSrv.dll with the following IDL stub information:

```
// opcode: 0x00, address: 0x65741030
// uuid: 25288888-bd5b-11d1-9d53-0080c83a5c2c
// version: 1.0
```

```
error_status_t rpc_opnum_0 (
[in] handle_t arg_1,
[in] long trend_req_num,
[in][size_is(arg_4)] byte overflow_str[],
[in] long arg_4,
[out][size_is(arg_6)] byte arg_5[],
[in] long arg_6
);
```

The upper half of the 'trend\_req\_num' DWORD RPC argument from above is used within TmRpcSrv.dll as an index into a call table. It must specifically be 0x0003 which results in a call to StRpcSrv.65671000(). The original arguments to the RPC endpoint are then passed to this called routine:

```
657416E6 mov eax, opnum0_call_table[eax*4]
657416ED test eax, eax
657416EF jnz short loc_65741707
...
65741707 loc_65741707:
65741707 mov [ebp+var_4], 0
6574170E mov edx, [ebp+sizeof_arg5]
65741711 push edx
65741712 mov edx, [ebp+arg5_array]
65741715 push edx
65741716 mov edx, [ebp+sizeof_overflow_str]
65741719 push edx
6574171A mov edx, [ebp+overflow_str]
6574171D push edx
6574171E push ecx ; trend_req_num
6574171F call eax ; call handler
```

The lower half of the 'trend\_req\_num' DWORD RPC argument is then used within StRpcSrv.dll as an index into a second call table. The value of this lower half controls the code flow to the following vulnerabilities and is hereto referred to as the 'subcode'.

### Vulnerability One:

A subcode value of 0x0004 results in a call to ENG\_SetRealTimeScanConfigInfo() which subsequently calls through Eng50.61181940() -> Eng50.611819E0() -> Eng50.61190F60() and can result in a stack overflow due to an unbounded widechar string copy into a ~600 byte stack-based buffer as shown in the following relevant excerpt:

## [NEWS] Trend Micro ServerProtect eng50.dll Stack Overflow Vulnerabilities

```
61190FC7 lea edx, [esp+288h+szShortPath]
61190FCB push esi
61190FCC push edx
61190FCD call _wcscpy
```

### Vulnerability Two:

A subcode value of 0x0047 results in a call to ENG\_SendEMail() which can result in a stack overflow due to an unbounded widechar string copy into a ~2k stack-based buffer as shown in the following relevant excerpt:

```
6118A161 mov esi, [esp+780h+arg_0]
6118A168 lea eax, [esp+780h+var_778]
6118A16C push esi
6118A16D push eax
6118A16E call _wcscpy
```

The resulting stack overflows can be leveraged to execute arbitrary code under the privileges of the SYSTEM user.

### Vendor Response:

Trend Micro has issued an update to correct this vulnerability. More details can be found at:

<<http://esupport.trendmicro.com/support/viewxml.do?ContentID=EN-1034290>>  
<http://esupport.trendmicro.com/support/viewxml.do?ContentID=EN-1034290>

### Disclosure Timeline:

2007.02.01 – Vulnerability reported to vendor  
2007.01.16 – Digital Vaccine released to TippingPoint customers  
2007.02.20 – Coordinated public release of advisory

## ADDITIONAL INFORMATION

The information has been provided by TippingPoint Security Research Team.

The original article can be found at:

<<http://www.tippingpoint.com/security/advisories/TSRT-07-02.html>>  
<http://www.tippingpoint.com/security/advisories/TSRT-07-02.html>

=====

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@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.