

[UNIX] Multiple Unauthenticated Stack Overflows in Asterisk Chan_sip.c (STP)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2007-07/msg00008.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxx>
 - *Date:* 5 Jul 2007 13:23:13 +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>

Multiple Unauthenticated Stack Overflows in Asterisk Chan_sip.c (STP)

SUMMARY

Two closely related stack based buffer overflows exist in the SIP/SDP handler of Asterisk, the vulnerabilities are very similar but exist as two separate unsafe function calls. The T38FaxRateManagement and T38FaxUdpEC SDP parameters can be exploited remotely leading to arbitrary code execution without authentication. In order for these overflows to occur, t38 fax over SIP must be enabled in sip.conf.

Examples of SIP INVITE packets are shown in the details section, however these vulnerabilities can be triggered with a number of different SIP messages affecting calls received by Asterisk, or in response to calls made by Asterisk.

DETAILS

Vulnerable Systems:

- * Asterisk versions prior to 1.4.3
- * AsteriskNOW versions prior to Beta6
- * Asterisk Appliance Developers Kits versions prior to 0.4.0

[UNIX] Multiple Unauthenticated Stack Overflows in Asterisk Chan_sip.c (STP)

Remote Unauthenticated stack overflow in Asterisk SIP/SDP T38FaxRateManagement parameter

A remote unauthenticated stack overflow exists in the SIP/SDP handler of Asterisk. By sending a SIP packet with SDP data which includes an overly long T38 parameter it is possible to overflow a stack based buffer and execute arbitrary code.

The process_sdp function of chan_sip.c in Asterisk contains the following vulnerable call to sscanf.

```
else if ((sscanf(a, "T38FaxRateManagement:%s", s) == 1)) {
found = 1;
if (option_debug > 2)

ast_log(LOG_DEBUG, "RateMangement: %s\n", s);
if (!strcasecmp(s, "localTCF"))
peert38capability |=
T38FAX_RATE_MANAGEMENT_LOCAL_TCF;
else if (!strcasecmp(s, "transferredTCF"))
peert38capability |=
T38FAX_RATE_MANAGEMENT_TRANSFERED_TCF;
```

This attempts to read the "T38FaxRateManagement:" option from the SDP within a SIP packet and copy the succeeding string into "s". There are no checks on the length of this string and we can therefore write past the boundaries of the "s" variable overwriting adjacent memory on the stack. "s" is defined earlier in this function as being a character array of only 256 bytes.

The following example packet demonstrates an overflow of this parameter:

```
INVITE sip:200@xxxxxxxx SIP/2.0
Date: Wed, 21 Mar 2007 4:20:09 GMT
CSeq: 1 INVITE
Via: SIP/2.0/UDP
10.0.0.123:5068;branch=z9hG4bKfe06f452-2dd6-db11-6d02-000b7d0dc672;rport
User-Agent: NGS/2.0
From: "Barrie Dempster"
<sip:zeedo@xxxxxxxx:5068>;tag=de92d852-2dd6-db11-9d02-000b7d0dc672
Call-ID: f897d952-2fa6-db49441-9d02-001b7d0dc672@hades
To: <sip:200@localhost>
Contact: <sip:zeedo@xxxxxxxx:5068;transport=udp>
Allow: INVITE,ACK,OPTIONS,BYE,CANCEL,NOTIFY,REFER,MESSAGE
Content-Type: application/sdp
Content-Length: 796
Max-Forwards: 70
```

```
v=0
o=rtsp 1160124458839569000 160124458839569000 IN IP4 127.0.0.1
s=-
c=IN IP4 127.0.0.1
```


[UNIX] Multiple Unauthenticated Stack Overflows in Asterisk Chan_sip.c (STP)

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

In order to subscribe to the mailing list, simply forward this email to: 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.