



August, 2007

McAfee, Inc.
McAfee® Avert® Labs Security Advisory
Public Release Date: 2007-08-27

Asterisk Skinny channel driver remote crash vulnerability
CVE-2007-4280

- **Synopsis**

Asterisk is the most popular and extensible open source telephone system in the world, offering flexibility, functionality and features not available in advanced, high cost proprietary business systems.

A vulnerability has been discovered in various Asterisk products, which could be exploited by remote attackers to cause a denial of service.

- **Vulnerable System or Application**

Asterisk Open Source versions prior to 1.4.10
AsteriskNOW versions prior to beta7
Asterisk Appliance Developer Kit versions prior to 0.7.0
Asterisk Appliance s800i versions prior to 1.0.3

- **Vulnerability Information**

This issue is caused by an error in the Skinny channel driver (chan_skinny) when processing a "CAPABILITIES_RES_MESSAGE" packet with a capabilities count greater than the total number of items in the "capabilities_res_message" array. This could be exploited by remote authenticated attackers to crash a vulnerable application, creating a denial of service condition.

channels/chan_skinny.c

```
3399 static int handle_capabilities_res_message(struct skinny_req *req, struct skinny_session *s)
3400 {
3401     struct skinny_device *d = s->device;
3402     struct skinny_line *l;
3403     int count = 0;
3404     int codecs = 0;
3405     int i;
3406
3407     count = leohl(req->data.caps.count);
3408
3409     for (i = 0; i < count; i++) {
```

```
3410     int acodec = 0;
3411     int scodec = 0;
3412     scodec = letohl(req->data.caps.caps[i].codec);
3413     acodec = codec_skinny2ast(scodec);
3414     if (skinnydebug)
3415         ast_verbose("Adding codec capability %d (%d)\n", acodec, scodec);
3416     codecs |= acodec;
3417 }
```

Line 3407, count is user controlled without proper bounds checking. So line 3412 will trigger a crash if the count is large.

- **Resolution**

Please update the software

Upgrade to Asterisk version 1.4.10 :
<ftp://ftp.digium.com/pub/telephony/asterisk>

Upgrade to AsteriskNOW beta7 :
<http://www.asterisknow.org>

Upgrade to Asterisk Appliance Developer Kit version 0.7.0 :
<ftp://ftp.digium.com/pub/telephony/aadk/>

Upgrade to Asterisk Appliance s800i version 1.0.3 :
<http://www.digium.com/en/supportcenter/>

- **Credits**

The vulnerability was discovered by Wei Wang of McAfee Avert Labs.

- **Legal Notice**

Copyright (C) 2007 McAfee, Inc.

The information contained within this advisory is provided for the convenience of McAfee's customers, and may be redistributed provided that no fee is charged for distribution and that the advisory is not modified in any way. McAfee makes no representations or warranties regarding the accuracy of the information referenced in this document, or the suitability of that information for your purposes.

McAfee, Inc. and McAfee Avert Labs are registered Trademarks of McAfee, Inc. and/or its affiliated companies in the United States and/or other Countries. All other registered and unregistered trademarks in this document are the sole property of their respective owners.