Product	Asterisk
Summary	Resource Exhaustion vulnerability in IAX2 channel driver
Nature of Advisory	Denial of Service
Susceptibility	Remote Unauthenticated Sessions
Severity	Moderate
Exploits Known	No
Reported On	July 19, 2007
Reported By	Russell Bryant, Digium, Inc. <russell@digium.com>
Posted On	July 23, 2007
Last Updated On	August 21, 2007
Advisory Contact	Russell Bryant <russell@digium.com>
CVE Name	CVE-2007-4103

Description	The IAX2 channel driver in Asterisk is vulnerable to a Denial of Service attack when configured to allow unauthenticated calls. An attacker can send a flood of NEW packets for valid extensions to the server to initiate calls as the unauthenticated user. This will cause resources on the Asterisk system to get allocated that will never go away. Furthermore, the IAX2 channel driver will be stuck trying to reschedule retransmissions for each of these fake calls forever. This can very quickly bring down a system and the only way to recover is to restart Asterisk. Detailed Explanation: Within the last few months, we made some changes to chan_iax2 to combat the abuse of this module for traffic amplification attacks. Unfortunately, this has caused an unintended side effect. The summary of the change to combat traffic amplification is this. Once you start the PBX on the Asterisk channel, it will begin receiving frames to be sent back out to the network. We delayed this from happening until a 3-way handshake has occurred to help ensure that we are talking to the IP address the messages appear to be coming from. When chan_iax2 accepts an unauthenticated call, it immediately creates the ast_channel for the call. However, since the 3-way handshake has not been completed, the PBX is not started on this channel. Later, when the maximum number of retries have been exceeded on responses to this NEW, the code tries to hang up the call. Now, it has 2 ways to do this, depending on if there is an ast_channel related to this IAX2 session or not. If there is no channel, then it can just destroy the iax2 private structure and move on. If there is a channel, it queues a HANGUP frame, and expects that to make the

	ast_channel get torn down, which would then cause the pvt struct to get destroyed afterwords. However, since there was no PBX started on this channel, there is nothing servicing the channel to receive the HANGUP frame. Therefore, the call never gets destroyed. To make things worse, there is some code continuously rescheduling PINGs and LAGRQs to be sent for the active IAX2 call, which will always fail. In summary, sending a bunch of NEW frames to request unauthenticated calls can make a server unusable within a matter of seconds.

Resolution	The default configuration that is distributed with Asterisk includes a guest account that allows unauthenticated calls. If this account and any other account without a password is disabled for IAX2, then the system is not vulnerable to this problem. For systems that continue to allow unauthenticated IAX2 calls, they must be updated to one of the versions listed as including the fix below.

Affected Versions		
Product	**Release Series**	
Asterisk Open Source	1.0.x	Not affected
Asterisk Open Source	1.2.x	1.2.20, 1.2.21, 1.2.21.1, 1.2.22
Asterisk Open Source	1.4.x	1.4.5, 1.4.6, 1.4.7, 1.4.7.1, 1.4.8
Asterisk Business Edition	A.x.x	Not affected
Asterisk Business Edition	B.x.x	Not affected
AsteriskNOW	pre-release	beta6
Asterisk Appliance Developer Kit	0.x.x	0.5.0
s800i (Asterisk Appliance)	1.0.x	1.0.0-beta5 up to and including 1.0.2

Corrected In	
Product	**Release**
Asterisk Open Source	1.2.23 and 1.4.9, available for download from http://downloads.digium.com/pub/asterisk
AsteriskNOW	Beta6, available from http://www.asterisknow.org/. Users can update using the system update feature in the appliance control panel.
Asterisk Appliance Developer Kit	0.6.0, available for download from http://downloads.digium.com/pub/aadk
s800i (Asterisk Appliance)	1.0.3

Links	

Asterisk Project Security Advisories are posted at http://www.asterisk.org/security.
This document may be superseded by later versions; if so, the latest version will be posted at http://downloads.digium.com/pub/asa/AST-2007-018.pdf.

Revision History		
Date	**Editor**	**Revisions Made**
July 23, 2007	russell@digium.com	Initial Release
August 1, 2007	russell@digium.com	Added CVE Name
August 21, 2007	russell@digium.com	Changed name prefix from ASA to AST, changed ftp.digium.com to downloads.digium.com