Product	Asterisk
Summary	Resource Exhaustion vulnerability in SIP channel driver
Nature of Advisory	Denial of Service
Susceptibility	Remote Unauthenticated Sessions
Severity	Moderate
Exploits Known	No
Reported On	August 9, 2007
Reported By	Jon Moldenauer (bugs.digium.com user jmoldenhauer)
Posted On	August 21, 2007
Last Updated On	August 21, 2007
Advisory Contact	Russell Bryant <russell@digium.com>
CVE Name	CVE-2007-4455

Description	The handling of SIP dialog history was broken during the development of Asterisk 1.4. Regardless of whether recording SIP dialog history is turned on or off, the history is still recorded in memory. Furthermore, there is no upper limit on how many history items will be stored for a given SIP dialog. It is possible for an attacker to use up all of the system's memory by creating a SIP dialog that records many entires in the history and never ends. It is also worth noting for the sake of doing the math to calculate what it would take to exploit this that each SIP history entry will take up a maximum of 88 bytes.

Resolution	The fix that has been added to chan_sip is to restore the functionality where SIP dialog history is not recorded in memory if it is not enabled. Furthermore, a maximum of 50 entires in the history will be stored for each dialog when recording history is turned on. The only way to avoid this problem in affected versions of Asterisk is to disable chan_sip. If chan_sip is being used, the system must be upgraded to a version that has this issue resolved.

Affected Versions

Product	Release Series	
Asterisk Open Source	1.0.x	Not affected
Asterisk Open Source	1.2.x	Not affected
Asterisk Open Source	1.4.x	All versions prior to 1.4.11
Asterisk Business Edition	A.x.x	Not affected
Asterisk Business Edition	B.x.x	Not affected
AsteriskNOW	pre-release	All versions prior to beta7
Asterisk Appliance Developer Kit	0.x.x	All versions prior to 0.8.0
s800i (Asterisk Appliance)	1.0.x	All versions prior to 1.0.3

Corrected In

Product	Release
Asterisk Open Source	1.4.11, available from http://downloads.digium.com/pub/telephony/asterisk
AsteriskNOW	Beta7, available from http://www.asterisknow.org/. Beta5 and Beta6 users can update using the system update feature in the appliance control panel.
Asterisk Appliance Developer Kit	0.8.0, available from http://downloads.digium.com/pub/telephony/aadk
s800i (Asterisk Appliance)	1.0.3

Links	http://bugs.digium.com/view.php?id=10421 http://bugs.digium.com/view.php?id=10418

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-2007-020.pdf and http://downloads.digium.com/pub/asa/AST-2007-020.html.

Revision History		
Date	**Editor**	**Revisions Made**
August 21, 2007	russell@digium.com	Initial Release