Product	Asterisk
Summary	Remote Crash Vulnerability in SIP channel driver
Nature of Advisory	Denial of Service
Susceptibility	Remote Unauthenticated Sessions
Severity	Critical in 1.6.1; minor in lesser versions
Exploits Known	No
Reported On	July 28, 2009
Reported By	Nick Baggott < nbaggott AT mudynamics DOT com >
Posted On	August 10, 2009
Last Updated On	August 13, 2009
Advisory Contact	Tilghman Lesher < tlesher AT digium DOT com >
CVE Name	CVE-2009-2726

Description	On certain implementations of libc, the scanf family of functions uses an unbounded amount of stack memory to repeatedly allocate string buffers prior to conversion to the target type. Coupled with Asterisk's allocation of thread stack sizes that are smaller than the default, an attacker may exhaust stack memory in the SIP stack network thread by presenting excessively long numeric strings in various fields. Note that while this potential vulnerability has existed in Asterisk for a very long time, it is only potentially exploitable in 1.6.1 and above, since those versions are the first that have allowed SIP packets to exceed 1500 bytes total, which does not permit strings that are large enough to crash Asterisk. (The number strings presented to us by the security researcher were approximately 32,000 bytes long.) Additionally note that while this can crash Asterisk, execution of arbitrary code is not possible with this vector.

Resolution	Upgrade Asterisk to one of the releases listed below.

Affected Versions		
Product	**Release Series**	
Asterisk Open Source	1.2.x	All versions prior to 1.2.34
Asterisk Open Source	1.4.x	All versions prior to 1.4.26.1
Asterisk Open Source	1.6.0.x	All versions prior to 1.6.0.13
Asterisk Open Source	1.6.1.x	All versions prior to 1.6.1.4
Asterisk Addons	1.2.x	Not affected
Asterisk Addons	1.4.x	Not affected
Asterisk Addons	1.6.0.x	Not affected
Asterisk Addons	1.6.1.x	Not affected
Asterisk Business Edition	A.x.x	All versions
Asterisk Business Edition	B.x.x	All versions prior to B.2.5.9
Asterisk Business Edition	C.2.x	All versions prior to C.2.4.1
Asterisk Business Edition	C.3.x	All versions prior to C.3.1
AsteriskNOW	1.5	Not affected
s800i (Asterisk Appliance)	1.2.x	All versions prior to 1.3.0.3

Corrected In	
Product	**Release**
Asterisk Open Source	1.2.34
Asterisk Open Source	1.4.26.1
Asterisk Open Source	1.6.0.13
Asterisk Open Source	1.6.1.4
Asterisk Business Edition	B.2.5.9
Asterisk Business Edition	C.2.4.1
Asterisk Business Edition	C.3.1
s800i (Asterisk Appliance)	1.3.0.3

Patches	
Link	**Branch**
http://downloads.digium.com/pub/security/AST-2009-005-1.2.diff.txt	1.2
http://downloads.digium.com/pub/security/AST-2009-005-1.4.diff.txt	1.4
http://downloads.digium.com/pub/security/AST-2009-005-trunk.diff.txt	trunk
http://downloads.digium.com/pub/security/AST-2009-005-1.6.0.diff.txt	1.6.0
http://downloads.digium.com/pub/security/AST-2009-005-1.6.1.diff.txt	1.6.1
http://downloads.digium.com/pub/security/AST-2009-005-1.6.2.diff.txt	1.6.2

Links	http://labs.mudynamics.com/advisories/MU-200908-01.txt

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/security/AST-2009-005.pdf and http://downloads.digium.com/pub/security/AST-2009-005.html

Revision History		
Date	**Editor**	**Revisions Made**
August 10, 2009	Tilghman Lesher	Initial release
August 13, 2009	Tilghman Lesher	Changed 1.6.0 version to 1.6.0.13