Product	Asterisk
Summary	Stack buffer overflow in SIP channel driver
Nature of Advisory	Exploitable Stack Buffer Overflow
Susceptibility	Remote Authenticated Sessions
Severity	Moderate
Exploits Known	No
Reported On	January 11, 2011
Reported By	Matthew Nicholson
Posted On	January 18, 2011
Last Updated On	January 20, 2011
Advisory Contact	Matthew Nicholson <mnicholson@digium.com>
CVE Name	CVE-2011-0495

Description	When forming an outgoing SIP request while in pedantic mode, a stack buffer can be made to overflow if supplied with carefully crafted caller ID information. This vulnerability also affects the URIENCODE dialplan function and in some versions of asterisk, the AGI dialplan application as well. The ast_uri_encode function does not properly respect the size of its output buffer and can write past the end of it when encoding URIs.

Resolution	The size of the output buffer passed to the ast_uri_encode function is now properly respected. In asterisk versions not containing the fix for this issue, limiting strings originating from remote sources that will be URI encoded to a length of 40 characters will protect against this vulnerability. exten => s,1,Set(CALLERID(num)=${CALLERID(num):0:40}) exten => s,n,Set(CALLERID(name)=${CALLERID(name):0:40}) exten => s,n,Dial(SIP/channel) The CALLERID(num) and CALLERID(name) channel values, and any strings passed to the URIENCODE dialplan function should be limited in this manner.

Affected Versions		
Product	**Release Series**	
Asterisk Open Source	1.2.x	All versions
Asterisk Open Source	1.4.x	All versions
Asterisk Open Source	1.6.x	All versions
Asterisk Open Source	1.8.x	All versions
Asterisk Business Edition	C.x.x	All versions
AsteriskNOW	1.5	All versions
s800i (Asterisk Appliance)	1.2.x	All versions

Corrected In	
Product	**Release**
Asterisk Open Source	1.4.38.1, 1.4.39.1, 1.6.1.21, 1.6.2.15.1, 1.6.2.16.1, 1.8.1.2, 1.8.2.2
Asterisk Business Edition	C.3.6.2

Patches	
URL	**Branch**
http://downloads.asterisk.org/pub/security/AST-2011-001-1.4.diff	1.4
http://downloads.asterisk.org/pub/security/AST-2011-001-1.6.1.diff	1.6.1
http://downloads.asterisk.org/pub/security/AST-2011-001-1.6.2.diff	1.6.2
http://downloads.asterisk.org/pub/security/AST-2011-001-1.8.diff	1.8

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This document may be superseded by later versions; if so, the latest version will be posted at http://downloads.digium.com/pub/security/AST-2011-001.pdf and http://downloads.digium.com/pub/security/AST-2011-001.html

Revision History		
Date	**Editor**	**Revisions Made**
2011-01-18	Matthew Nicholson	Initial Release
2011-01-19	Matthew Nicholson	Added CVE Name
2011-01-20	Matthew Nicholson	Changed 1.8.2.1 to 1.8.2.2 for fix versions

Asterisk Project Security Advisory - AST-2011-001