Product	Asterisk
Summary	Buffer Overflow Exploit Through SIP SDP Header
Nature of Advisory	Exploitable Stack Buffer Overflow
Susceptibility	Remote Unauthenticated Sessions
Severity	Major
Exploits Known	No
Reported On	6 January, 2013
Reported By	Ulf Härnhammar
Posted On	27 March, 2013
Last Updated On	March 27, 2013
Advisory Contact	Jonathan Rose <jrose AT digium DOT com>
CVE Name	CVE-2013-2685

Description	The format attribute resource for h264 video performs an unsafe read against a media attribute when parsing the SDP. The vulnerable parameter can be received as strings of an arbitrary length and Asterisk attempts to read them into limited buffer spaces without applying a limit to the number of characters read. If a message is formed improperly, this could lead to an attacker being able to execute arbitrary code remotely.

Resolution	Attempts to read string data into the buffers noted are now explicitly limited by the size of the buffers.

Affected Versions		
Product	**Release Series**	
Asterisk Open Source	11.x	All Versions

Corrected In	
Product	**Release**
Asterisk Open Source	11.2.2

Patches	
SVN URL	**Revision**
Http://downloads.asterisk.org/pub/security/AST-2013-001-11.diff	Asterisk 11

Links	https://issues.asterisk.org/jira/browse/ASTERISK-20901

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This document may be superseded by later versions; if so, the latest version will be posted at http://downloads.digium.com/pub/security/AST-2013-001.pdf and http://downloads.digium.com/pub/security/AST-2013-001.html

Revision History		
Date	**Editor**	**Revisions Made**
February 11, 2013	Jonathan Rose	Initial Draft
March 27, 2013	Matt Jordan	CVE Added