Product	Asterisk
Summary	Remote Crash Vulnerability in Milliwatt Application
Nature of Advisory	Exploitable Stack Buffer Overflow with locally defined data
Susceptibility	Remote Unauthenticated Sessions
Severity	Minor
Exploits Known	No
Reported On	03/14/2012
Reported By	Russell Bryant
Posted On	03/15/2012
Last Updated On	March 15, 2012
Advisory Contact	Matt Jordan <mjordan AT digium DOT com>
CVE Name	

Description	An attacker can cause Asterisk to crash in one of two ways: 1. A dialplan uses the Milliwatt application with 'o' option 2. The internal_timing option in asterisk.conf is off 3. The attacker sends a large audio packet. The number of samples in the audio packet determines the number of internal data samples that are copied into the buffer. This overruns the buffer, potentially causing a crash. OR 1. A dialplan uses the Milliwatt application with the 'o' option 2. The attacker negotiates a media format with a sampling rate greater than 32kHz. The application will attempt to generate an audio packet using the sample rate of the negotiated format, where the sample rate will require a number of data points greater then the size of the buffer. Again, the the application copies a number of internal data samples into the buffer that are greater then the size of the buffer, potentially causing a crash. Note that the latter attack vector is only possible in Asterisk 10, as it supports codecs with a sample rate greater then 32kHz.

Resolution	Upgrade to one of the versions of Asterisk listed in the “Corrected In” section, or apply a patch specified in the “Patches” section.

Affected Versions		
Product	**Release Series**	
Asterisk Open Source	1.4.x	All Versions
Asterisk Open Source	1.6.2.x	All Versions
Asterisk Open Source	1.8.x	All Versions
Asterisk Open Source	10.x	All Versions

Corrected In	
Product	**Release**
Asterisk Open Source	1.4.44
Asterisk Open Source	1.6.2.23
Asterisk Open Source	1.8.10.1
Asterisk Open Source	10.2.1

Patches	
SVN URL	**Revision**
http://downloads.asterisk.org/pub/security/AST-2012-002-1.4.diff	v1.4
http://downloads.asterisk.org/pub/security/AST-2012-002-1.6.2.diff	v1.6.2
http://downloads.asterisk.org/pub/security/AST-2012-002-1.8.diff	v1.8
http://downloads.asterisk.org/pub/security/AST-2012-002-10.diff	v10

Links	https://issues.asterisk.org/jira/browse/ASTERISK-19541

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This document may be superseded by later versions; if so, the latest version will be posted at http://downloads.digium.com/pub/security/AST-2012-002.pdf and http://downloads.digium.com/pub/security/AST-2012-002.html

Revision History		
Date	**Editor**	**Revisions Made**
03/15/2012	Matt Jordan	Initial Release
03/16/2012	Matt Jordan	Correct links, typos