Product	Asterisk
Summary	Remote crash vulnerability in IAX2 channel driver.
Nature of Advisory	Remote crash
Susceptibility	Established calls
Severity	Moderate
Exploits Known	No
Reported On	March 21, 2012
Reported By	mgrobecker
Posted On	May 29, 2012
Last Updated On	May 29, 2012
Advisory Contact	Richard Mudgett < rmudgett AT digium DOT com >
CVE Name	CVE-2012-2947

Description	A remotely exploitable crash vulnerability exists in the IAX2 channel driver if an established call is placed on hold without a suggested music class. For this to occur, the following must take place: 1. The setting mohinterpret=passthrough must be set on the end placing the call on hold. 2. A call must be established. 3. The call is placed on hold without a suggested music-on-hold class name. When these conditions are true, Asterisk will attempt to use an invalid pointer to a music-on-hold class name. Use of the invalid pointer will either cause a crash or the music-on-hold class name will be garbage.

Resolution	Asterisk now sets the extra data parameter to null if the received control frame does not have any extra data.

Affected Versions		
Product	**Release Series**	
Certified Asterisk	1.8.11-cert	All versions
Asterisk Open Source	1.8.x	All versions
Asterisk Open Source	10.x	All versions

Corrected In	
Product	**Release**
Certified Asterisk	1.8.11-cert2
Asterisk Open Source	1.8.12.1, 10.4.1

Patches	
SVN URL	**Revision**
http://downloads.asterisk.org/pub/security/AST-2012-007-1.8.11-cert.diff	v1.8.11-cert
http://downloads.asterisk.org/pub/security/AST-2012-007-1.8.diff	v1.8
http://downloads.asterisk.org/pub/security/AST-2012-007-10.diff	v10

Links	https://issues.asterisk.org/jira/browse/ASTERISK-19597

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This document may be superseded by later versions; if so, the latest version will be posted at http://downloads.digium.com/pub/security/AST-2012-007.pdf and http://downloads.digium.com/pub/security/AST-2012-007.html

Revision History		
Date	**Editor**	**Revisions Made**
05/29/2012	Richard Mudgett	Initial release.