Product	Asterisk
Summary	Multiple array overflow and crash vulnerabilities in UDPTL code
Nature of Advisory	Exploitable Stack and Heap Array Overflows
Susceptibility	Remote Unauthenticated Sessions
Severity	Critical
Exploits Known	No
Reported On	January 27, 2011
Reported By	Matthew Nicholson
Posted On	February 21, 2011
Last Updated On	March 11, 2011
Advisory Contact	Matthew Nicholson <mnicholson@digium.com>
CVE Name	CVE-2011-1147

Description	When decoding UDPTL packets, multiple stack and heap based arrays can be made to overflow by specially crafted packets. Systems configured for T.38 pass through or termination are vulnerable.

Resolution	The UDPTL decoding routines have been modified to respect the limits of exploitable arrays. In asterisk versions not containing the fix for this issue, disabling T.38 support will prevent this vulnerability from being exploited. T.38 support can be disabled in chan_sip by setting the t38pt_udptl option to “no” (it is off by default). t38pt_udptl = no The chan_ooh323 module should also be disabled by adding the following line in modles.conf. noload => chan_ooh323

Affected Versions		
Product	**Release Series**	
Asterisk Open Source	1.4.x	All versions
Asterisk Open Source	1.6.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	1.4.39.2, 1.6.1.22, 1.6.2.16.2, 1.8.2.4
Asterisk Business Edition	C.3.6.3

Patches	
URL	**Branch**
http://downloads.asterisk.org/pub/security/AST-2011-002-1.4.diff	1.4
http://downloads.asterisk.org/pub/security/AST-2011-002-1.6.1.diff	1.6.1
http://downloads.asterisk.org/pub/security/AST-2011-002-1.6.2.diff	1.6.2
http://downloads.asterisk.org/pub/security/AST-2011-002-1.8.diff	1.8

Links	

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This document may be superseded by later versions; if so, the latest version will be posted at http://downloads.digium.com/pub/security/AST-2011-002.pdf and http://downloads.digium.com/pub/security/AST-2011-002.html

Revision History		
Date	**Editor**	**Revisions Made**
02/21/11	Matthew Nicholson	Initial Release
02/22/11	Matthew Nicholson	Changed some wording
03/11/11	Matthew Nicholson	Added CVE Name