Product	Asterisk
Summary	T.38 Remote Crash Vulnerability
Nature of Advisory	Denial of Service
Susceptibility	Remote unauthenticated sessions
Severity	Critical
Exploits Known	No
Reported On	12/03/09
Reported By	issues.asterisk.org users bklang and elsto
Posted On	02/03/10
Last Updated On	February 2, 2010
Advisory Contact	David Vossel < dvossel AT digium DOT com >
CVE Name	CVE-2010-0441

Description	An attacker attempting to negotiate T.38 over SIP can remotely crash Asterisk by modifying the FaxMaxDatagram field of the SDP to contain either a negative or exceptionally large value. The same crash occurs when the FaxMaxDatagram field is omitted from the SDP as well.

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	1.6.x	All versions
Asterisk Business Edition	C.3	All versions

Corrected In	
Product	**Release**
Asterisk Open Source	1.6.0.22
Asterisk Open Source	1.6.1.14
Asterisk Open Source	1.6.2.2
	C.3.3.2

Patches	
SVN URL	**Branch**
http://downloads.asterisk.org/pub/security/AST-2010-001-1.6.0.diff	v1.6.0
http://downloads.asterisk.org/pub/security/AST-2010-001-1.6.1.diff	v1.6.1
http://downloads.asterisk.org/pub/security/AST-2010-001-1.6.2.diff	v1.6.2

Links	https://issues.asterisk.org/view.php?id=16634 https://issues.asterisk.org/view.php?id=16724 https://issues.asterisk.org/view.php?id=16517

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This document may be superseded by later versions; if so, the latest version will be posted at http://downloads.digium.com/pub/security/.pdf and http://downloads.digium.com/pub/security/.html

Revision History		
Date	**Editor**	**Revisions Made**
02/02/10	David Vossel	Initial release