Product	Asterisk
Summary	Database matching order permits host-based authentication to be ignored
Nature of Advisory	Logic error
Susceptibility	Remote Unauthenticated Sessions
Severity	Moderate
Exploits Known	No
Reported On	October 30, 2007
Reported By	Tilghman Lesher <tlesher AT digium DOT com>
Posted On	December 18, 2007
Last Updated On	December 18, 2007
Advisory Contact	Tilghman Lesher <tlesher AT digium DOT com>
CVE Name	CVE-2007-6430

Description	Due to the way database-based registrations (“realtime”) are processed, IP addresses are not checked when the username is correct and there is no password. An attacker may impersonate any user using host-based authentication without a secret, simply by guessing the username of that user. This is limited in scope to administrators who have set up the registration database (“realtime”) for authentication and are using only host-based authentication, not passwords. However, both the SIP and IAX protocols are affected.

Resolution	As a workaround, administrators may set a password for all users and peers in their registration “realtime” database. A fix is included in the newest release of Asterisk, as provided below.

Affected Versions		
Product	**Release Series**	
Asterisk Open Source	1.0.x	Not affected
Asterisk Open Source	1.2.x	All versions prior to 1.2.26
Asterisk Open Source	1.4.x	All versions prior to 1.4.16
Asterisk Business Edition	A.x.x	Not affected
Asterisk Business Edition	B.x.x	All versions prior to B.2.3.6
Asterisk Business Edition	C.x.x	All versions prior to C.1.0-beta8
AsteriskNOW	pre-release	Not affected
Asterisk Appliance Developer Kit	0.x.x	Not affected
s800i (Asterisk Appliance)	1.0.x	Not affected

Corrected In	
Product	**Release**
Asterisk Open Source	1.2.26
Asterisk Open Source	1.4.16
Asterisk Business Edition	B.2.3.6
Asterisk Business Edition	C.1.0-beta8

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This document may be superseded by later versions; if so, the latest version will be posted at http://downloads.digium.com/pub/security/AST-2007-027.pdf and http://downloads.digium.com/pub/security/AST-2007-027.html

Revision History		
Date	**Editor**	**Revisions Made**
2007-12-18	Tilghman Lesher	Initial Release