Product	Asterisk
Summary	SIP responses expose valid usernames
Nature of Advisory	Information leak
Susceptibility	Remote Unauthenticated Sessions
Severity	Minor
Exploits Known	No
Reported On	October 26, 2009
Reported By	Patrik Karlsson <patrik AT cqure DOT net>
Posted On	November 4, 2009
Last Updated On	November 10, 2009
Advisory Contact	Joshua Colp <jcolp AT digium DOT com>
CVE Name	CVE-2009-3727

Description	It is possible to determine if a peer with a specific name is configured in Asterisk by sending a specially crafted REGISTER message twice. The username that is to be checked is put in the user portion of the URI in the To header. A bogus non-matching value is put into the username portion of the Digest in the Authorization header. If the peer does exist the second REGISTER will receive a response of “403 Authentication user name does not match account name”. If the peer does not exist the response will be “404 Not Found” if alwaysauthreject is disabled and “401 Unauthorized” if alwaysauthreject is enabled.

Resolution	Upgrade to one of the versions below, or apply one of the patches specified in the Patches section.

Affected Versions		
Product	**Release Series**	
Asterisk Open Source	1.2.x	All versions prior to 1.2.35
Asterisk Open Source	1.4.x	All versions prior to 1.4.26.3
Asterisk Open Source	1.6.0.x	All versions prior to 1.6.0.17
Asterisk Open Source	1.6.1.x	All versions prior to 1.6.1.9
Asterisk Addons	1.2.x	Unaffected
Asterisk Addons	1.4.x	Unaffected
Asterisk Addons	1.6.x	Unaffected
Asterisk Business Edition	A.x.x	All versions
Asterisk Business Edition	B.x.x	All versions prior to B.2.5.12
Asterisk Business Edition	C.x.x	All versions prior to C.2.4.5 and C.3.2.2
AsteriskNOW	1.5	All versions
s800i (Asterisk Appliance)	1.2.x	All versions prior to 1.3.0.5

Corrected In	
Product	**Release**
Asterisk Open Source	1.2.35
Asterisk Open Source	1.4.26.3
Asterisk Open Source	1.6.0.17
Asterisk Open Source	1.6.1.9
Asterisk Business Edition	B.2.5.12
Asterisk Business Edition	C.2.4.5
Asterisk Business Edition	C.3.2.2
S800i (Asterisk Appliance)	1.3.0.5

Patches	
SVN URL	**Revision**
http://downloads.digium.com/pub/asa/AST-2009-008-1.2.diff.txt	1.2
http://downloads.digium.com/pub/asa/AST-2009-008-1.4.diff.txt	1.4
http://downloads.digium.com/pub/asa/AST-2009-008-1.6.0.diff.txt	1.6.0

http://downloads.digium.com/pub/asa/AST-2009-008-1.6.1.diff.txt	1.6.1

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-2009-008.pdf and http://downloads.digium.com/pub/security/AST-2009-008.html

Revision History		
Date	**Editor**	**Revisions Made**
November 4, 2009	Joshua Colp	Initial release
November 10, 2009	Joshua Colp	Added CVE assignment