Product	Asterisk
Summary	Possible enumeration of SIP users due to differing authentication responses
Nature of Advisory	Unauthorized data disclosure
Susceptibility	Remote unauthenticated sessions
Severity	Moderate
Exploits Known	No
Reported On	June 11, 2011
Reported By	
Posted On	June 28, 2011
Last Updated On	June 28, 2011
Advisory Contact	Terry Wilson <twilson@digium.com>
CVE Name	CVE-2011-2536

Description	Asterisk may respond differently to SIP requests from an invalid SIP user than it does to a user configured on the system, even when the alwaysauthreject option is set in the configuration. This can leak information about what SIP users are valid on the Asterisk system.

Resolution	Respond to SIP requests from invalid and valid SIP users in the same way. Asterisk 1.4 and 1.6.2 do not respond identically by default due to backward-compatibility reasons, and must have alwaysauthreject=yes set in sip.conf. Asterisk 1.8 defaults to alwaysauthreject=yes. IT IS ABSOLUTELY IMPERATIVE that users of Asterisk 1.4 and 1.6.2 set alwaysauthreject=yes in the general section of sip.conf.

Affected Versions		
Product	**Release Series**	
Asterisk Open Source	1.4.x	All versions
Asterisk Open Source	1.6.2.x	All versions
Asterisk Open Source	1.8.x	All versions
Asterisk Business Edition	C.3.x	All versions

Corrected In	
Product	**Release**
Asterisk Open Source	1.4.41.2, 1.6.2.18.2, 1.8.4.4
Asterisk Business Edition	C.3.7.3

Patches	
Download URL	**Revision**
http://downloads.asterisk.org/pub/security/AST-2011-011-1.4.diff	1.4
http://downloads.asterisk.org/pub/security/AST-2011-011-1.6.2.diff	1.6.2
http://downloads.asterisk.org/pub/security/AST-2011-011-1.8.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This document may be superseded by later versions; if so, the latest version will be posted at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-2011-011.pdf and
http://downloads.digium.com/pub/security/AST-2011-011.html

Revision History		
Date	**Editor**	**Revisions Made**