Product	Asterisk
Summary	SIP responses expose valid usernames
Nature of Advisory	Information leak
Susceptibility	Remote Unauthenticated Sessions
Severity	Minor
Exploits Known	No
Reported On	February 23, 2009
Reported By	Gentoo Linux Project: Kerin Millar (kerframil on irc.freenode.net) and Fergal Glynn < FGlynn AT veracode DOT com >
Posted On	April 2, 2009
Last Updated On	April 2, 2009
Advisory Contact	Tilghman Lesher < tlesher AT digium DOT com >
CVE Name	CVE-2008-3903

Description	In 2006, the Asterisk maintainers made it more difficult to scan for valid SIP usernames by implementing an option called "alwaysauthreject", which should return a 401 error on all replies which are generated for users which do not exist. While this was sufficient at the time, due to ever increasing compliance with RFC 3261, the SIP specification, that is no longer sufficient as a means towards preventing attackers from checking responses to verify whether a SIP account exists on a machine. What we have done is to carefully emulate exactly the same responses throughout possible dialogs, which should prevent attackers from gleaning this information. All invalid users, if this option is turned on, will receive the same response throughout the dialog, as if a username was valid, but the password was incorrect. It is important to note several things. First, this vulnerability is derived directly from the SIP specification, and it is a technical violation of RFC 3261 (and subsequent RFCs, as of this date), for us to return these responses. Second, this attack is made much more difficult if administrators avoided creating all-numeric usernames and especially all-numeric passwords. This combination is extremely vulnerable for servers connected to the public Internet, even with this patch in place. While it may make configuring SIP telephones easier in the short term, it has the potential to cause grief over the long term.

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 1.2.32
Asterisk Open Source	1.4.x	All versions prior to 1.4.24.1
Asterisk Open Source	1.6.0.x	All versions prior to 1.6.0.8
Asterisk Addons	1.2.x	Not affected
Asterisk Addons	1.4.x	Not affected
Asterisk Addons	1.6.x	Not affected
Asterisk Business Edition	A.x.x	All versions
Asterisk Business Edition	B.x.x	All versions prior to B.2.5.8
Asterisk Business Edition	C.1.x.x	All versions prior to C.1.10.5
Asterisk Business Edition	C.2.x.x	All versions prior to C.2.3.3
AsteriskNOW	1.5	Not affected
s800i (Asterisk Appliance)	1.3.x	All versions prior to 1.3.0.2

Corrected In	
Product	**Release**
Asterisk Open Source	1.2.32
Asterisk Open Source	1.4.24.1
Asterisk Open Source	1.6.0.8
Asterisk Business Edition	B.2.5.8
Asterisk Business Edition	C.1.10.5
Asterisk Business Edition	C.2.3.3
s800i (Asterisk Appliance)	1.3.0.2

Patches	
Patch URL	**Version**
http://downloads.digium.com/pub/asa/AST-2009-003-1.2.diff.txt	1.2
http://downloads.digium.com/pub/asa/AST-2009-003-1.4.diff.txt	1.4
http://downloads.digium.com/pub/asa/AST-2009-003-1.6.0.diff.txt	1.6.0
http://downloads.digium.com/pub/asa/AST-2009-003-1.6.1.diff.txt	1.6.1

Links	http://www.faqs.org/rfcs/rfc3261.html

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-2009-003.pdf and http://downloads.digium.com/pub/security/AST-2009-003.html

Revision History		
Date	**Editor**	**Revisions Made**
2009-04-02	Tilghman Lesher	Initial release