Product	Asterisk
Summary	Information leak in IAX2 authentication
Nature of Advisory	Unauthorized data disclosure
Susceptibility	Remote Unauthenticated Sessions
Severity	Minor
Exploits Known	Yes
Reported On	October 15, 2008
Reported By	http://www.unprotectedhex.com
Posted On	January 7, 2009
Last Updated On	June 4, 2009
Advisory Contact	Tilghman Lesher < tlesher AT digium DOT com >
CVE Name	CVE-2009-0041

Description	IAX2 provides a different response during authentication when a user does not exist, as compared to when the password is merely wrong. This allows an attacker to scan a host to find specific users on which to concentrate password cracking attempts. The workaround involves sending back responses that are valid for that particular site. For example, if it were known that a site only uses RSA authentication, then sending back an MD5 authentication request would similarly identify the user as not existing. The opposite is also true. So the solution is always to send back an authentication response that corresponds to a known frequency with which real authentication responses are returned, when the user does not exist. This makes it very difficult for an attacker to guess whether a user exists or not, based upon this particular mechanism. Additionally, it's worth noting that the simplistic method used to scan for usernames is made much more difficult if usernames consisted of more than simply numeric digits. Also, the ability to scan for usernames in this manner is serious only if administrators insist upon using numeric passwords, which are similarly easy to scan for matches. Once an attacker has been able to verify a username and password by scanning, then fraudulent activity may commence with the same rights as the scanned user. As this is unlikely to be the last of many scanners, administrators would be well advised to guard against insecure VoIP passwords on their systems.

Resolution	Upgrade to revision 199157 of the 1.2 branch, 199138 of the 1.4 branch, 199142 of the 1.6.0 branch, 199141 of the 1.6.1 branch, or one of the releases noted below.

Affected Versions		
Product	**Release Series**	
Asterisk Open Source	1.2.x	All version prior to 1.2.3.1
Asterisk Open Source	1.4.x	All versions prior to 1.4.25.1
Asterisk Open Source	1.6.x	All versions prior to 1.6.0.10
Asterisk Open Source	1.6.x	All versions prior to 1.6.1.1
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.2.5.7
Asterisk Business Edition	C.1.x.x	All versions prior to C.1.10.4
Asterisk Business Edition	C.2.x.x	All versions prior to C.2.1.2.1
AsteriskNOW	1.5	Not affected
s800i (Asterisk Appliance)	1.2.x	All versions prior to 1.3.1

Corrected In	
Product	**Release**
Asterisk Open Source	1.2.33
Asterisk Open Source	1.4.25.1
Asterisk Open Source	1.6.0.10
Asterisk Open Source	1.6.1.1
Asterisk Business Edition	B.2.5.7
Asterisk Business Edition	C.1.10.4
Asterisk Business Edition	C.2.1.2.1
s800i (Asterisk Appliance)	1.3.1

Patches	
URL	**Branch**
http://downloads.asterisk.org/pub/security/AST-2009-001-1.2.patch	1.2

http://downloads.asterisk.org/pub/security/AST-2009-001-1.4.patch	1.4
http://downloads.asterisk.org/pub/security/AST-2009-001-1.6.0.patch	1.6.0
http://downloads.asterisk.org/pub/security/AST-2009-001-1.6.1.patch	1.6.1

Links	http://code.google.com/p/iaxscan/

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.asterisk.org/pub/security/AST-2009-001.pdf and http://downloads.asterisk.org/pub/security/AST-2009-001.html

Revision History		
Date	**Editor**	**Revisions Made**
2009-01-07	Tilghman Lesher	Initial release
2009-01-12	Tilghman Lesher	Modified patches, added section about poor password choices
2009-01-23	Tilghman Lesher	Updated version numbers
2009-05-29	Tilghman Lesher	Updated patches
2009-06-04	David Vossel	Updated patches, affected revision numbers, added 1.6.1 release to advisory, updated links to reflect asterisk.org domain change.