Product	Asterisk
Summary	Invalid parsing of ACL rules can compromise security
Nature of Advisory	Unauthorized access to system
Susceptibility	Remote Unauthenticated Sessions
Severity	Moderate
Exploits Known	No
Reported On	Feb 24, 2010
Reported By	Mark Michelson
Posted On	Feb 25, 2010
Last Updated On	February 25, 2010
Advisory Contact	Mark Michelson < mmichelson AT digium DOT com >
CVE Name	

Description	Host access rules using "permit=" and "deny=" configurations behave unpredictably if the CIDR notation "/0" is used. Depending on the system's behavior, this may act as desired, but in other cases it might not, thereby allowing access from hosts that should be denied. Note that even if an unauthorized host is allowed access due to this exploit, authentication measures still in place would prevent further unauthorized access. Note also that there is a workaround for this problem, which is to use the dotted-decimal format "/0.0.0.0" instead of CIDR notation. The bug does not exist when using this format. In addition, this format is what is used in Asterisk's sample configuration files.

Resolution	Code has been corrected to behave consistently on all systems when "/0" is used.

Affected Versions		
Product	**Release Series**	
Asterisk Open Source	1.2.x	Unaffected
Asterisk Open Source	1.4.x	Unaffected
Asterisk Open Source	1.6.x	All 1.6.0, 1.6.1 and 1.6.2 releases
Asterisk Addons	1.2.x	Unaffected
Asterisk Addons	1.4.x	Unaffected
Asterisk Addons	1.6.x	Unaffected
Asterisk Business Edition	A.x.x	Unaffected
Asterisk Business Edition	B.x.x	Unaffected
Asterisk Business Edition	C.x.x	Unaffected
AsteriskNOW	1.5	Unaffected
s800i (Asterisk Appliance)	1.2.x	Unaffected

Corrected In	
Product	**Release**
Asterisk	1.6.0.25
Asterisk	1.6.1.17
Asterisk	1.6.2.5

Patches	
URL	**Branch**
http://downloads.asterisk.org/pub/security/AST-2010-003-1.6.0.diff	1.6.0
http://downloads.asterisk.org/pub/security/AST-2010-003-1.6.1.diff	1.6.1
http://downloads.asterisk.org/pub/security/AST-2010-003-1.6.2.diff	1.6.2

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This document may be superseded by later versions; if so, the latest version will be posted at http://downloads.digium.com/pub/security/AST-2010-003.pdf and http://downloads.digium.com/pub/security/AST-2010-003.html

Revision History		
Date	**Editor**	**Revisions Made**
Feb 24, 2010	Mark Michelson	Initial Advisory