Product	Asterisk
Summary	Mixed IP address families in access control lists may permit unwanted traffic.
Nature of Advisory	Unauthorized Access
Susceptibility	Remote unauthenticated sessions
Severity	Moderate
Exploits Known	No
Reported On	25 October, 2014
Reported By	Andreas Steinmetz
Posted On	20 November, 2014
Last Updated On	November 21, 2014
Advisory Contact	Mark Michelson <mmichelson AT digium DOT com>
CVE Name	CVE-2014-8412

Description	Many modules in Asterisk that service incoming IP traffic have ACL options (“permit” and “deny”) that can be used to whitelist or blacklist address ranges. A bug has been discovered where the address family of incoming packets is only compared to the IP address family of the first entry in the list of access control rules. If the source IP address for an incoming packet is not of the same address family as the first ACL entry, that packet bypasses all ACL rules. For ACLs whose rules are all of the same address family, there is no issue. Note that while the incoming packet may bypass ACL rules, the packet is still subject to any authentication requirements that the specific protocol employs. This issue affects the following parts of Asterisk • All VoIP channel drivers • DUNDi • Asterisk Manager Interface (AMI)

Resolution	The ACL code has been amended to compare the incoming packet's source address family against the address families for all rules.

Affected Versions		
Product	**Release Series**	
Asterisk Open Source	1.8.x	All versions
Asterisk Open Source	11.x	All versions
Asterisk Open Source	12.x	All versions
Asterisk Open Source	13.x	All versions
Certified Asterisk	1.8.28	All versions
Certified Asterisk	11.6	All versions

Corrected In	
Product	**Release**
Asterisk Open Source	1.8.32.1, 11.14.1, 12.7.1, 13.0.1
Certified Asterisk	1.8.28-cert3, 11.6-cert8

Patches	
SVN URL	**Revision**
http://downloads.asterisk.org/pub/security/AST-2014-012-1.8.diff	Asterisk 1.8
http://downloads.asterisk.org/pub/security/AST-2014-012-1.8.28.diff	Certified Asterisk 1.8.28
http://downloads.asterisk.org/pub/security/AST-2014-012-11.diff	Asterisk 11
http://downloads.asterisk.org/pub/security/AST-2014-012-11.6.diff	Certified Asterisk 11.6
http://downloads.asterisk.org/pub/security/AST-2014-012-12.diff	Asterisk 12
http://downloads.asterisk.org/pub/security/AST-2014-012-13.diff	Asterisk 13

Links	https://issues.asterisk.org/jira/browse/ASTERISK-24469

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-2014-012.pdf and http://downloads.digium.com/pub/security/AST-2014-012.html

Revision History		
Date	**Editor**	**Revisions Made**
5 November, 2014	Mark Michelson	Initial Advisory created