

## Asterisk Project Security Advisory - AST-2012-013

<b>Product</b>	Asterisk
<b>Summary</b>	ACL rules ignored when placing outbound calls by certain IAX2 users
<b>Nature of Advisory</b>	Unauthorized use of system
<b>Susceptibility</b>	Remote Authenticated Sessions
<b>Severity</b>	Moderate
<b>Exploits Known</b>	None
<b>Reported On</b>	07/27/2012
<b>Reported By</b>	Alan Frisch
<b>Posted On</b>	08/30/2012
<b>Last Updated On</b>	August 31, 2012
<b>Advisory Contact</b>	Matt Jordan < mjordan AT digium DOT com >
<b>CVE Name</b>	CVE-2012-4737

<b>Description</b>	When an IAX2 call is made using the credentials of a peer defined in a dynamic Asterisk Realtime Architecture (ARA) backend, the ACL rules for that peer are not applied to the call attempt. This allows for a remote attacker who is aware of a peer's credentials to bypass the ACL rules set for that peer.
--------------------	---

<b>Resolution</b>	The ACL rules for peers defined in an ARA backend are now honored. Users of chan_ix2 should upgrade to the corrected versions; apply a provided patch; or define their IAX2 peers outside of an ARA backend in a static configuration file.
-------------------	---

<b>Affected Versions</b>		
<b>Product</b>	<b>Release Series</b>	
Asterisk Open Source	1.8.x	All versions
Asterisk Open Source	10.x	All versions
Certified Asterisk	1.8.11	All versions
Asterisk Digiumphones	10.x.x- digiumphones	All versions
Asterisk Business Edition	C.3.x	All versions

## Asterisk Project Security Advisory - AST-2012-013

Copyright © 2012 Digium, Inc. All Rights Reserved.

Permission is hereby granted to distribute and publish this advisory in its original, unaltered form.

## Asterisk Project Security Advisory - AST-2012-013

<b>Corrected In</b>	
<b>Product</b>	<b>Release</b>
Asterisk Open Source	1.8.15.1, 10.7.1
Certified Asterisk	1.8.11-cert7
Asterisk Digiumphones	10.7.1-digiumphones
Asterisk Business Edition	C.3.7.6

<b>Patches</b>	
<b>SVN URL</b>	<b>Revision</b>
<a href="http://downloads.asterisk.org/pub/security/AST-2012-013-1.8.diff">http://downloads.asterisk.org/pub/security/AST-2012-013-1.8.diff</a>	Asterisk 1.8
<a href="http://downloads.asterisk.org/pub/security/AST-2012-013-10.diff">http://downloads.asterisk.org/pub/security/AST-2012-013-10.diff</a>	Asterisk 10

<b>Links</b>	<a href="https://issues.asterisk.org/jira/browse/ASTERISK-20186">https://issues.asterisk.org/jira/browse/ASTERISK-20186</a>
--------------	---

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-2012-013.pdf> and <http://downloads.digium.com/pub/security/AST-2012-013.html>

<b>Revision History</b>		
<b>Date</b>	<b>Editor</b>	<b>Revisions Made</b>
08/27/2012	Matt Jordan	Initial Revision
08/31/2012	Matt Jordan	Updated patch links

Asterisk Project Security Advisory - AST-2012-013

Copyright © 2012 Digium, Inc. All Rights Reserved.

Permission is hereby granted to distribute and publish this advisory in its original, unaltered form.