

## Asterisk Project Security Advisory - AST-2007-015

<b>Product</b>	Asterisk
<b>Summary</b>	Remote Crash Vulnerability in IAX2 channel driver
<b>Nature of Advisory</b>	Denial of Service
<b>Susceptibility</b>	Remote Unauthenticated Sessions
<b>Severity</b>	Critical
<b>Exploits Known</b>	No
<b>Reported On</b>	July 13, 2007
<b>Reported By</b>	Chris Clark and Zane Lackey, iSEC Partners
<b>Posted On</b>	July 17, 2007
<b>Last Updated On</b>	August 21, 2007
<b>Advisory Contact</b>	Russell Bryant <russell@digium.com>
<b>CVE Name</b>	CVE-2007-3763

<b>Description</b>	<p>The Asterisk IAX2 channel driver, chan_ix2, has a remotely exploitable crash vulnerability. A NULL pointer exception can occur when Asterisk receives a LAGRQ or LAGRP frame that is part of a valid session and includes information elements. The session used to exploit this issue does not have to be authenticated. It can simply be a NEW packet sent with an invalid username.</p> <p>The code that parses the incoming frame correctly parses the information elements of IAX frames. It then sets a pointer to NULL to indicate that there is not a raw data payload associated with this frame. However, it does not set the variable that indicates the number of bytes in the raw payload back to zero. Since the raw data length is non-zero, the code handling LAGRQ and LAGRP frames tries to copy data from a NULL pointer, causing a crash.</p>
--------------------	--

<b>Resolution</b>	All users that have chan_ix2 enabled should upgrade to the appropriate version listed in the corrected in section of this advisory.
-------------------	---

## Asterisk Project Security Advisory - AST-2007-015

Copyright © 2007 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-2007-015

<b>Affected Versions</b>		
<b>Product</b>	<b>Release Series</b>	
Asterisk Open Source	1.0.x	All versions
Asterisk Open Source	1.2.x	All versions prior to 1.2.22
Asterisk Open Source	1.4.x	All versions prior to 1.4.8
Asterisk Business Edition	A.x.x	All versions
Asterisk Business Edition	B.x.x	All versions prior to B.2.2.1
AsteriskNOW	pre-release	All versions prior to beta7
Asterisk Appliance Developer Kit	0.x.x	All versions prior to 0.5.0
s800i (Asterisk Appliance)	1.0.x	All versions prior to 1.0.2

<b>Corrected In</b>	
<b>Product</b>	<b>Release</b>
Asterisk Open Source	1.2.22 and 1.4.8, available from <a href="http://downloads.digium.com/pub/telephony/asterisk">http://downloads.digium.com/pub/telephony/asterisk</a>
Asterisk Business Edition	B.2.2.1, available from the Asterisk Business Edition user portal on <a href="http://www.digium.com">http://www.digium.com</a> or via Digium Technical Support
AsteriskNOW	Beta7, available from <a href="http://www.asterisknow.org/">http://www.asterisknow.org/</a> . Beta5 and Beta6 users can update using the system update feature in the appliance control panel.
Asterisk Appliance Developer Kit	0.5.0, available from <a href="http://downloads.digium.com/pub/telephony/aadk/">http://downloads.digium.com/pub/telephony/aadk/</a>
s800i (Asterisk Appliance)	1.0.2

<b>Links</b>

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/asa/AST-2007-015.pdf> and <http://downloads.digium.com/pub/asa/AST-2007-015.html>.

<b>Revision History</b>

Asterisk Project Security Advisory - AST-2007-015

Copyright © 2007 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-2007-015

<b>Date</b>	<b>Editor</b>	<b>Revisions Made</b>
July 17, 2007	russell@digium.com	Initial Release
August 21, 2007	russell@digium.com	Changed name prefix from ASA to AST, changed <a href="http://ftp.digium.com">ftp.digium.com</a> to <a href="http://downloads.digium.com">downloads.digium.com</a>

Asterisk Project Security Advisory - AST-2007-015

Copyright © 2007 Digium, Inc. All Rights Reserved.

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