

Asterisk Project Security Advisory - AST-2008-001

Product	Asterisk
Summary	Remote Crash Vulnerability in SIP channel driver
Nature of Advisory	Denial of Service
Susceptibility	Remote Unauthenticated Sessions
Severity	Critical
Exploits Known	No
Reported On	December 26, 2007
Reported By	Grey VoIP (bugs.digium.com user greyvoip)
Posted On	January 2, 2008
Last Updated On	January 2, 2008
Advisory Contact	Joshua Colp <jcolp@digium.com>
CVE Name	

Description	The handling of the BYE with Also transfer method was broken during the development of Asterisk 1.4. If a transfer attempt is made using this method the system will immediately crash upon handling the BYE message due to trying to copy data into a NULL pointer. It is important to note that a dialog must have already been established and up in order for this to happen.
--------------------	---

Resolution	A fix has been added so that the BYE with Also transfer method now properly allocates and uses the transfer data structure. It will no longer try to copy data into a NULL pointer and will operate properly.
-------------------	---

Asterisk Project Security Advisory - AST-2008-001

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-2008-001

Affected Versions		
Product	Release Series	
Asterisk Open Source	1.0.x	Unaffected
Asterisk Open Source	1.2.x	Unaffected
Asterisk Open Source	1.4.x	All versions prior to 1.4.17
Asterisk Business Edition	A.x.x	Unaffected
Asterisk Business Edition	B.x.x	Unaffected
Asterisk Business Edition	C.x.x	All versions prior to C.1.0-beta8
AsteriskNOW	pre-release	All versions prior to beta7
Asterisk Appliance Developer Kit	SVN	All versions prior to Asterisk 1.4 revision 95946
s800i (Asterisk Appliance)	1.0.x	All versions prior to 1.0.3.4

Corrected In	
Product	Release
Asterisk Open Source	1.4.17, available from http://downloads.digium.com/pub/telephony/asterisk
Asterisk Business Edition	C.1.0
AsteriskNOW	Beta7, available from http://www.asterisknow.org/ . Beta5 and Beta6 users can update using the system update feature in the appliance control panel.
Asterisk Appliance Developer Kit	Asterisk 1.4 revision 95946. Available by performing an svn update of the AADK tree.
s800i (Asterisk Appliance)	1.0.3.4

Links	http://bugs.digium.com/view.php?id=11637
--------------	---

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-2008-001.pdf> and <http://downloads.digium.com/pub/security/AST-2008-001.html>

Revision History

Asterisk Project Security Advisory - AST-2008-001

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-2008-001

Date	Editor	Revisions Made
2008-01-02	Joshua Colp	Initial Release

Asterisk Project Security Advisory - AST-2008-001

Copyright © 2007 Digium, Inc. All Rights Reserved.

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