

Asterisk Project Security Advisory - AST-2008-009

Product	Asterisk-Addons
Summary	Remote crash vulnerability in ooh323 channel driver
Nature of Advisory	Remote crash
Susceptibility	Remote unauthenticated sessions
Severity	Major
Exploits Known	No
Reported On	May 29, 2008
Reported By	Tzafrir Cohen <tzafrir DOT cohen AT xorcom DOT com>
Posted On	June 4, 2008
Last Updated On	June 4, 2008
Advisory Contact	Mark Michelson <mmichelson AT digium DOT com>
CVE Name	CVE-2008-2543

Description	The ooh323 channel driver provided in Asterisk Addons used a TCP connection to pass commands internally. The payload of these packets included addresses of memory which were to be freed after the command was processed. By sending arbitrary data to the listening TCP socket, one could cause an almost certain crash since the command handler would attempt to free invalid memory. This problem was made worse by the fact that the listening TCP socket was bound to whatever IP address was specified by the "bindaddr" option in ooh323.conf
--------------------	--

Resolution	The TCP connection used by ooh323 has been replaced with a pipe. The effect of this change is that data from outside the ooh323 process may not be injected.
-------------------	--

Asterisk Project Security Advisory - AST-2008-009

Copyright © 2008 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-2008-009

Affected Versions		
Product	Release Series	
Asterisk Open Source	1.0.x	N/A
Asterisk Open Source	1.2.x	N/A
Asterisk Open Source	1.4.x	N/A
Asterisk Addons	1.2.x	All versions prior to 1.2.9
Asterisk Addons	1.4.x	All versions prior to 1.4.7
Asterisk Business Edition	A.x.x	N/A
Asterisk Business Edition	B.x.x	N/A
Asterisk Business Edition	C.x.x	N/A
AsteriskNOW	pre-release	N/A
Asterisk Appliance Developer Kit	0.x.x	N/A
s800i (Asterisk Appliance)	1.0.x	N/A

Corrected In	
Product	Release
Asterisk Addons 1.2	1.2.9
Asterisk-Addons 1.4	1.4.7

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 This document may be superseded by later versions; if so, the latest version will be posted at 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-2008-009.pdf> and <http://downloads.digium.com/pub/security/AST-2008-009.html>

Revision History		
Date	Editor	Revisions Made
Jun 3, 2008	Mark Michelson	Initial draft

Asterisk Project Security Advisory - AST-2008-009

Copyright © 2008 Digium, Inc. All Rights Reserved.

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