Asterisk Project Security Advisory - AST-2009-002

Product	Asterisk
Summary	Remote Crash Vulnerability in SIP channel driver
Nature of Advisory	Denial of Service
Susceptibility	Remote Authenticated Sessions
Severity	Moderate
Exploits Known	No
Reported On	February 6, 2009
Reported By	bugs.digium.com user klaus3000
Posted On	March 10, 2009
Last Updated On	March 10, 2009
Advisory Contact	Joshua Colp <jcolp@digium.com>
CVE Name	

Description	When configured with pedantic=yes the SIP channel driver performs extra request URI checking on an INVITE received as a result of a SIP spiral. As part of this extra checking the headers from the outgoing SIP INVITE sent and the received SIP INVITE are compared. The code incorrectly assumes that the string for each header passed in will be non-NULL in all cases. This is incorrect because if no headers are present the value passed in will be NULL. The values passed into the code are now checked to be non-NULL before being compared.

Resolution	Upgrade to revision 174082 of the 1.4 branch, 174085 of the 1.6.0 branch, 174086 of the 1.6.1 branch, or one of the releases noted below. The pedantic option in the SIP channel driver can also be turned off to prevent this issue from occurring.

Affected Versions

Product	Release Series	
Asterisk Open Source	1.2.x	Not affected
Asterisk Open Source	1.4.x	Versions 1.4.22, 1.4.23, 1.4.23.1
Asterisk Open Source	1.6.0.x	All versions prior to 1.6.0.6
Asterisk Open Source	1.6.1.x	All versions prior to 1.6.1.0-rc2
Asterisk Addons	1.2.x	Not affected
Asterisk Addons	1.4.x	Not affected
Asterisk Addons	1.6.x	Not affected
Asterisk Business Edition	A.x.x	Not affected
Asterisk Business Edition	B.x.x	Not affected
Asterisk Business Edition	C.x.x	Only version C.2.3
s800i (Asterisk Appliance)	1.2.x	Not affected

Corrected In

Product	Release
Asterisk Open Source	1.4.23.2
Asterisk Open Source	1.6.0.6
Asterisk Open Source	1.6.1.0-rc2
Asterisk Business Edition	C.2.3.2

Patches

URL	Branch
http://downloads.digium.com/pub/security/AST-2009-002-1.4.diff	1.4
http://downloads.digium.com/pub/security/AST-2009-002-1.6.0.diff	1.6.0
http://downloads.digium.com/pub/security/AST-2009-002-1.6.1.diff	1.6.1

Links	http://bugs.digium.com/view.php?id=14417 http://bugs.digium.com/view.php?id=13547

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This document may be superseded by later versions; if so, the latest version will be posted at http://downloads.digium.com/pub/security/AST-2009-002.pdf and http://downloads.digium.com/pub/security/AST-2009-002.html

Revision History		
Date	**Editor**	**Revisions Made**
2009-03-10	Joshua Colp	Initial release