Asterisk Project Security Advisory - AST-2008-002

Product	Asterisk
Summary	Two buffer overflows in RTP Codec Payload Handling
Nature of Advisory	Exploitable Buffer Overflow
Susceptibility	Remote Unauthenticated Sessions
Severity	Critical
Exploits Known	No
Reported On	March 11, 2008
Reported By	Mu Security Research Team
Posted On	March 18, 2008
Last Updated On	December 15, 2008
Advisory Contact	Joshua Colp <jcolp@digium.com>
CVE Name	CVE-2008-1289

Description	Two buffer overflows exist in the RTP payload handling code of Asterisk. Both overflows can be caused by an INVITE or any other SIP packet with SDP. The request may need to be authenticated depending on configuration of the Asterisk installation. The first overflow is caused by sending a payload number that surpasses the programmed maximum payload number of 256. This causes an invalid memory write outside of the buffer. While this does not allow the attacker to write arbitrary data it does allow the attacker to write a 0 to other memory locations. The second overflow is caused by sending more than 32 RTP payloads. This causes a buffer on the stack to overflow allowing the attacker to write values between 0 and 256 (the maximum payload number) to memory locations after the buffer.

Resolution	Two fixes have been added to check the provided data to ensure it does not exceed static buffer sizes. When removing internal information regarding an RTP payload the given payload number will now be checked to make sure it does not exceed the maximum acceptable payload number. When reading RTP payloads from SDP a maximum limit of 32 in total will be enforced. Any further RTP payloads will be discarded.

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 1.4.18.1 and 1.4.19-rc3
Asterisk Open Source	1.6.x	All versions prior to 1.6.0-beta6
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.1.6.1
AsteriskNOW	1.0.x	All versions prior to 1.0.2
Asterisk Appliance Developer Kit	SVN	All versions prior to Asterisk 1.4 revision 109386
s800i (Asterisk Appliance)	1.1.x	All versions prior to 1.1.0.2

Corrected In	
Product	**Release**
Asterisk Open Source	1.4.18.1/1.4.19-rc3/1.6.0-beta6, available from http://downloads.digium.com/pub/telephony/asterisk
Asterisk Business Edition	C.1.6.1
AsteriskNOW	1.0.2, available from http://www.asterisknow.org/ Current users can update using the system update feature in the appliance control panel.
Asterisk Appliance Developer Kit	Asterisk 1.4 revision 109386. Available by performing an svn update of the AADK tree.
s800i (Asterisk Appliance)	1.1.0.2

Patches	
URL	**Version**

http://downloads.digium.com/pub/security/AST-2008-002-1.4.patch	1.4
http://downloads.digium.com/pub/security/AST-2008-002-1.6.0.patch	1.6.0

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-2008-002.pdf and http://downloads.digium.com/pub/security/AST-2008-002.html

Revision History		
Date	**Editor**	**Revisions Made**
2008-03-18	Joshua Colp	Initial Release
2008-12-15	Joshua Colp	Add Patches