Product	Asterisk
Summary	Buffer overflows in voicemail when using IMAP storage
Nature of Advisory	Remotely and locally exploitable buffer overflows
Susceptibility	Remote Unauthenticated Sessions
Severity	Minor
Exploits Known	No
Reported On	October 9, 2007
Reported By	Russell Bryant <russell@digium.com> Mark Michelson <mmichelson@digium.com>
Posted On	October 9, 2007
Last Updated On	October 15, 2007
Advisory Contact	Mark Michelson <mmichelson@digium.com>
CVE Name	CVE-2007-5358

Description	The function “sprintf” was used heavily throughout the IMAP-specific voicemail code. After auditing the code, two vulnerabilities were discovered, both buffer overflows. The following buffer overflow required write access to Asterisk's configuration files in order to be exploited. 1) If a combination of the astspooldir (set in asterisk.conf), the voicemail context, and voicemail mailbox, were very long, then there was a buffer overflow when playing a message or forwarding a message (in the case of forwarding, the context and mailbox in question are the context and mailbox that the message was being forwarded to). The following buffer overflow could be exploited remotely. 2) If any one of, or any combination of the Content-type or Content-description headers for an e-mail that Asterisk recognized as a voicemail message contained more than a 1024 characters, then a buffer would overflow while listening to a voicemail message via a telephone. It is important to note that this did NOT affect users who get their voicemail via an e-mail client.

Resolution	“sprintf” calls have been changed to “snprintf” wherever space was not specifically allocated to the buffer prior to the sprintf call. This includes places which are not currently prone to buffer overflows.

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 1.4.13
Asterisk Business Edition	A.x.x	Unaffected
Asterisk Business Edition	B.x.x	Unaffected
AsteriskNOW	pre-release	Unaffected
Asterisk Appliance Developer Kit	0.x.x	Unaffected
s800i (Asterisk Appliance)	1.0.x	Unaffected

Corrected In	
Product	**Release**
Asterisk Open Source	1.4.13

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 This document may be superseded by later versions; if so, the latest version will be posted at http://downloads.digium.com/pub/security/AST-2007-022.pdf and http://downloads.digium.com/pub/security/AST-2007-022.html.

Revision History		
Date	**Editor**	**Revisions Made**
October 9, 2007	mmichelson@digium.com	Initial Release
October 15, 2007	mmichelson@digium.com	Added CVE name