Product	Zaptel
Summary	Potential buffer overflow from command line application “sethdlc”
Nature of Advisory	Buffer overflow
Susceptibility	Local sessions
Severity	None
Exploits Known	None
Reported On	October 31, 2007
Reported By	Michael Bucko <michael DOT bucko AT eleytt DOT com>
Posted On	October 31, 2007
Last Updated On	November 1, 2007
Advisory Contact	Mark Michelson <mmichelson AT digium DOT com>
CVE Name	CVE-2007-5690

Description	This advisory is a response to a false security vulnerability published in several places on the Internet. Had Asterisk's developers been notified prior to its publication, there would be no need for this. There is a potential for a buffer overflow in the sethdlc application; however, running this application requires root access to the server, which means that exploiting this vulnerability gains the attacker no more advantage than what he already has. As such, this is a bug, not a security vulnerability.

Resolution	The copy of the user-provided argument to the buffer has been limited to the length of the buffer. This fix has been committed to the Zaptel 1.2 and 1.4 repositories, but due to the lack of severity, new releases will not be immediately made. While we appreciate this programming error being brought to our attention, we would encourage security researchers to contact us prior to releasing any reports of their own, both so that we can fix any vulnerability found prior to the release of an announcement, as well as avoiding these types of mistakes (and the potential embarrassment of reporting a vulnerability that wasn't) in the future.

Affected Versions		
Product	**Release Series**	
Zaptel	1.2.x	All versions prior to 1.2.22
Zaptel	1.4.x	All versions prior to 1.4.7

Corrected In	
Product	**Release**
Zaptel	1.2.22, when available
Zaptel	1.4.7, when available

Links	http://archives.neohapsis.com/archives/bugtraq/2007-10/0316.html

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This document may be superseded by later versions; if so, the latest version will be posted at http://downloads.digium.com/pub/security/AST-2007-024.pdf and http://downloads.digium.com/pub/security/AST-2007-024.html.

Revision History		
Date	**Editor**	**Revisions Made**
10/31/2007	Mark Michelson	Initial release
10/31/2007	Mark Michelson	Changed severity, description, and resolution