Product	Asterisk
Summary	SQL Injection issue in cdr_pgsql
Nature of Advisory	SQL Injection
Susceptibility	Remote Authenticated Sessions
Severity	Moderate
Exploits Known	No
Reported On	November 29, 2007
Reported By	Tilghman Lesher <tlesher AT digium DOT com>
Posted On	November 29, 2007
Last Updated On	November 29, 2007
Advisory Contact	Tilghman Lesher <tlesher AT digium DOT com>
CVE Name	CVE-2007-6170

Description	Input buffers were not properly escaped when providing the ANI and DNIS strings to the Call Detail Record Postgres logging engine. An attacker could potentially compromise the administrative database containing users' usernames and passwords used for SIP authentication, among other things. This module is not active by default and must be configured for use by the administrator. Default installations of Asterisk are not affected.

Workaround	Convert your installation to use cdr_odbc with the PgsqlODBC driver. This module provides similar functionality but is not vulnerable.

Resolution	Upgrade to Asterisk release 1.4.15 or higher.

Affected Versions

Product	Release Series	
Asterisk Open Source	1.0.x	All versions
Asterisk Open Source	1.2.x	1.2.24 and previous
Asterisk Open Source	1.4.x	1.4.14 and previous
Asterisk Business Edition	A.x.x	All versions
Asterisk Business Edition	B.x.x	B.2.3.3 and previous
Asterisk Business Edition	C.x.x	C.1.0-beta5 and previous
AsteriskNOW	pre-release	None
Asterisk Appliance Developer Kit	0.x.x	None
s800i (Asterisk Appliance)	1.0.x	None

Corrected In

Product	Release
Asterisk Open Source	1.2.25
Asterisk Open Source	1.4.15
Asterisk Business Edition	B.2.3.4
Asterisk Business Edition	C.1.0-beta6

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This document may be superseded by later versions; if so, the latest version will be posted at http://downloads.digium.com/pub/security/AST-2007-026.pdf and http://downloads.digium.com/pub/security/AST-2007-026.html

Revision History

Date	Editor	Revisions Made
2007-11-29	Tilghman Lesher	Initial release
2007-11-29	Tilghman Lesher	Added CVE, ABE C version