Asterisk Project Security Advisory - AST-2007-023

Product	Asterisk-Addons
Summary	SQL Injection Vulnerability in cdr_addon_mysql
Nature of Advisory	SQL Injection
Susceptibility	Remote Unauthenticated Sessions
Severity	Minor
Exploits Known	Yes
Reported On	October 16, 2007
Reported By	Humberto Abdelnur <humberto.abdelnur AT loria DOT fr>
Posted On	October 16, 2007
Last Updated On	October 16, 2007
Advisory Contact	Tilghman Lesher <tlesher AT digium DOT com>
CVE Name	CVE-2007-5488

Description	The source and destination numbers for a given call are not correctly escaped by the cdr_addon_mysql module when inserting a record. Therefore, a carefully crafted destination number sent to an Asterisk system running cdr_addon_mysql could escape out of a SQL data field and create another query. This vulnerability is made all the more severe if a user were using realtime data, since the data may exist in the same database as the inserted call detail record, thus creating all sorts of possible data corruption and invalidation issues.

Resolution	The Asterisk-addons package is not distributed with Asterisk, nor is it installed by default. The module may be either disabled or upgraded to fix this issue.

Affected Versions

Product	Release Series	
Asterisk Open Source	1.0.x	All versions
Asterisk Open Source	1.2.x	All versions prior to asterisk-addons-1.2.8
Asterisk Open Source	1.4.x	All versions prior to asterisk-addons-1.4.4
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-Addons	1.2.8
Asterisk-Addons	1.4.4

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This document may be superseded by later versions; if so, the latest version will be posted at http://downloads.digium.com/pub/security/AST-2007-023.pdf and http://downloads.digium.com/pub/security/AST-2007-023.html.

Revision History

Date	Editor	Revisions Made
2007-10-16	Tilghman Lesher	Initial release
2007-10-16	Tilghman Lesher	Added CVE number