Product	Asterisk
Summary	func_odbc: Possible SQL Injection
Nature of Advisory	SQL injection
Susceptibility	Remote unauthenticated sessions
Severity	Low
Exploits Known	No
Reported On	January 5, 2022
Reported By	Leandro Dardini
Posted On	April 14, 2022
Last Updated On	April 12, 2022
Advisory Contact	Jcolp AT sangoma DOT com
CVE Name	CVE-2022-26651

Description	Some databases can use backslashes to escape certain characters, such as backticks. If input is provided to func_odbc which includes backslashes it is possible for func_odbc to construct a broken SQL query and the SQL query to fail. Additionally while it has not yet been reproduced this security advisory is also being published to cover the case of SQL injection with the aim of database manipulation by an outside party.
Modules Affected	func_odbc

Resolution	A new dialplan function, SQL_ESC_BACKSLASHES, has been added to the func_odbc module which will escape backslashes. If your usage of func_odbc may have input which includes backslashes and your database uses backslashes to escape backticks then use the dialplan function to escape the backslashes. A second option is to disable support for backslashes for escaping in your database if the underlying database supports it.

Affected Versions		
Product	**Release Series**	
Asterisk Open Source	16.x	All versions
Asterisk Open Source	18.x	All versions
Asterisk Open Source	19.x	All versions
Certified Asterisk	16.x	All versions

Corrected In	
Product	**Release**
Asterisk Open Source	16.25.2, 18.11.2, 19.3.2
Certified Asterisk	16.8-cert14

Patches	
Patch URL	**Revision**
https://downloads.digium.com/pub/security/AST-2022-003-16.diff	Asterisk 16
https://downloads.digium.com/pub/security/AST-2022-003-18.diff	Asterisk 18
https://downloads.digium.com/pub/security/AST-2022-003-19.diff	Asterisk 19
https://downloads.digium.com/pub/security/AST-2022-003-16.8.diff	Certified Asterisk 16.8

Links	https://issues.asterisk.org/jira/browse/ASTERISK-29838 https://downloads.asterisk.org/pub/security/AST-2022-003.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This document may be superseded by later versions; if so, the latest version will be posted at https://downloads.digium.com/pub/security/AST-2022-003.pdf and https://downloads.digium.com/pub/security/AST-2022-003.html

Revision History		
Date	**Editor**	**Revisions Made**

February 15, 2022	Joshua Colp	Initial revision