

AST-2007-023 – SQL Injection Vulnerability in cdr_addon_mysql

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/bugtraq/2007-10/msg00259.html>

- *From:* Asterisk Security Team <security@xxxxxxxxxxxxx>
 - *Date:* Tue, 16 Oct 2007 18:59:11 -0500
-

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 Leshner <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 |
+-----+
```

AST-2007-023 – SQL Injection Vulnerability in cdr_addon_mysql

| | 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 | A.x.x | Unaffected |
| Edition | | |

| Asterisk Business | B.x.x | Unaffected |
| Edition | | |

| AsteriskNOW | pre-release | Unaffected |

| Asterisk Appliance | 0.x.x | Unaffected |
| Developer Kit | | |

| s800i (Asterisk | 1.0.x | Unaffected |
| Appliance) | | |

| Corrected In |

| Product | Release |

| Asterisk-Addons | 1.2.8 |

| Asterisk-Addons | 1.4.4 |

AST-2007-023 – SQL Injection Vulnerabilty in cdr_addon_mysql

| 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 Leshner	Initial release
------------	------------------	-----------------

2007-10-16	Tilghman Leshner	Added CVE number
------------	------------------	------------------

Asterisk Project Security Advisory – 2007-AST-023

Copyright (c) 2007 Digium, Inc. All Rights Reserved.

Permission is hereby granted to distribute and publish this advisory in its original, unaltered form.