| | |
|---|---|
| **Product** | Asterisk |
| **Summary** | Buffer overflow in CDR's set user |
| **Nature of Advisory** | Buffer Overflow |
| **Susceptibility** | Remote Authenticated Sessions |
| **Severity** | Moderate |
| **Exploits Known** | No |
| **Reported On** | March 27, 2017 |
| **Reported By** | Alex Villacis Lasso |
| **Posted On** | |
| **Last Updated On** | April 14, 2017 |
| **Advisory Contact** | kharwell AT digium DOT com |
| **CVE Name** | CVE-2017-7617 |

| | |
|---|---|
| **Description** | No size checking is done when setting the user field on a CDR. Thus, it is possible for someone to use an arbitrarily large string and write past the end of the user field storage buffer. This allows the possibility of remote code injection.<br>This currently affects any system using CDR's that also make use of the following:<br>* The 'X-ClientCode' header within a SIP INFO message when using chan_sip and the 'useclientcode' option is enabled (note, it's disabled by default).<br>* The CDR dialplan function executed from AMI when setting the user field.<br>* The AMI Monitor action when using a long file name/path. |

| | |
|---|---|
| **Resolution** | The CDR engine now only copies up to the maximum allowed characters into the user field. Any characters outside the maximum are truncated. |

**Affected Versions**

| **Product** | **Release Series** | |
|---|---|---|
| Asterisk Open Source | 13.x | All Releases |
| Asterisk Open Source | 14.x | All Releases |
| Certified Asterisk | 13.13 | All Releases |

| **Corrected In** | |
|---|---|
| **Product** | **Release** |
| Asterisk Open Source | 13.14.1,14.3.1 |
| Certified Asterisk | 13.13-cert3 |

| **Patches** | |
|---|---|
| **SVN URL** | **Revision** |
| http://downloads.asterisk.org/pub/security/AST-2017-001-13.diff | Asterisk 13 |
| http://downloads.asterisk.org/pub/security/AST-2017-001-14.diff | Asterisk 14 |
| http://downloads.asterisk.org/pub/security/AST-2017-001-13.13.diff | Certified Asterisk 13.13 |

| | |
|---|---|
| **Links** | https://issues.asterisk.org/jira/browse/ASTERISK-26897 |

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This document may be superseded by later versions; if so, the latest version will be posted at http://downloads.digium.com/pub/security/AST-2017-001.pdf and http://downloads.digium.com/pub/security/AST-2017-001.html

| **Revision History** | | |
|---|---|---|
| **Date** | **Editor** | **Revisions Made** |
| March, 27, 2017 | Kevin Harwell | Initial Revision |
| April 14, 2017 | Joshua Colp | Added CVE |