| | |
|---|---|
| **Product** | Asterisk |
| **Summary** | Denial of Service Through File Descriptor Exhaustion with chan_sip Session-Timers |
| **Nature of Advisory** | Denial of Service |
| **Susceptibility** | Remote Authenticated or Anonymous Sessions |
| **Severity** | Moderate |
| **Exploits Known** | No |
| **Reported On** | 2014/02/25 |
| **Reported By** | Corey Farrell |
| **Posted On** | March 10, 2014 |
| **Last Updated On** | March 10, 2014 |
| **Advisory Contact** | Kinsey Moore <kmoore AT digium DOT com> |
| **CVE Name** | CVE-2014-2287 |

| | |
|---|---|
| **Description** | An attacker can use all available file descriptors using SIP INVITE requests.<br><br>Knowledge required to achieve the attack:<br>* Valid account credentials or anonymous dial in<br>* A valid extension that can be dialed from the SIP account<br><br>Trigger conditions:<br>* chan_sip configured with “session-timers” set to “originate” or “accept”<br>** The INVITE request must contain either a Session-Expires or a Min-SE header with malformed values or values disallowed by the system's configuration.<br>* chan_sip configured with “session-timers” set to “refuse”<br>** The INVITE request must offer “timer” in the “Supported” header<br><br>Asterisk will respond with code 400, 420, or 422 for INVITEs meeting this criteria. Each INVITE meeting these conditions will leak a channel and several file descriptors. The file descriptors cannot be released without restarting Asterisk which may allow intrusion detection systems to be bypassed by sending the requests slowly. |

| | |
|---|---|
| **Resolution** | Upgrade to a version with the patch integrated or apply the appropriate patch. |

| Affected Versions | | |
|---|---|---|
| **Product** | **Release Series** | |
| Asterisk Open Source | 1.8.x | All |
| Asterisk Open Source | 11.x | All |
| Asterisk Open Source | 12.x | All |
| Certified Asterisk | 1.8.15 | All |
| Certified Asterisk | 11.6 | All |

| Corrected In | |
|---|---|
| **Product** | **Release** |
| Asterisk Open Source 1.8.x | 1.8.26.1 |
| Asterisk Open Source 11.x | 11.8.1 |
| Asterisk Open Source 12.x | 12.1.1 |
| Certified Asterisk 1.8.15 | 1.8.15-cert5 |
| Certified Asterisk 11.6 | 11.6-cert2 |

| Patches | |
|---|---|
| **SVN URL** | **Revision** |
| http://downloads.asterisk.org/pub/security/AST-2014-002-1.8.diff | Asterisk 1.8 |
| http://downloads.asterisk.org/pub/security/AST-2014-002-11.diff | Asterisk 11 |
| http://downloads.asterisk.org/pub/security/AST-2014-002-12.diff | Asterisk 12 |
| http://downloads.asterisk.org/pub/security/AST-2014-002-11.6.diff | Asterisk 11.6 Certified |
| http://downloads.asterisk.org/pub/security/AST-2014-002-1.8.15.diff | Asterisk 1.8.15 Certified |

| **Links** | https://issues.asterisk.org/jira/browse/ASTERISK-23373 |
|---|---|

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-2014-002.pdf and http://downloads.digium.com/pub/security/AST-2014-002.html

| Revision History | | |
|---|---|---|
| **Date** | **Editor** | **Revisions Made** |
| 2014/03/04 | Kinsey Moore | Document Creation |
| 2014/03/06 | Kinsey Moore | Corrections and Wording Clarification |
| 2014/03/10 | Kinsey Moore | Added missing patch links |