Product	Asterisk
Summary	File descriptor exhaustion in chan_sip
Nature of Advisory	Denial of Service
Susceptibility	Remote Unauthenticated Sessions
Severity	Minor
Exploits Known	Yes
Reported On	September 17, 2015
Reported By	Alexander Traud
Posted On	February 3, 2016
Last Updated On	February 15, 2016
Advisory Contact	Richard Mudgett <rmudgett AT digium DOT com>
CVE Name	CVE-2016-2316

Description	Setting the sip.conf timert1 value to a value higher than 1245 can cause an integer overflow and result in large retransmit timeout times. These large timeout values hold system file descriptors hostage and can cause the system to run out of file descriptors.

Resolution	Setting the sip.conf timert1 value to 1245 or lower will not exhibit the vulnerability. The default timert1 value is 500. Asterisk has been patched to detect the integer overflow and calculate the previous retransmission timer value.

Affected Versions		
Product	**Release Series**	
Asterisk Open Source	1.8.x	All versions
Asterisk Open Source	11.x	All versions
Asterisk Open Source	12.x	All versions
Asterisk Open Source	13.x	All versions
Certified Asterisk	1.8.28	All versions
Certified Asterisk	11.6	All versions
Certified Asterisk	13.1	All versions

<table>
<tr><th colspan="2">Corrected In</th></tr>
<tr><th>Product</th><th>Release</th></tr>
<tr><td>Asterisk Open Source</td><td>11.21.1, 13.7.1</td></tr>
<tr><td>Certified Asterisk</td><td>11.6-cert12, 13.1-cert3</td></tr>
</table>

<table>
<tr><th colspan="2">Patches</th></tr>
<tr><th>SVN URL</th><th>Revision</th></tr>
<tr><td>http://downloads.asterisk.org/pub/security/AST-2016-002-1.8.28.diff</td><td>Certified Asterisk 1.8.28</td></tr>
<tr><td>http://downloads.asterisk.org/pub/security/AST-2016-002-11.6.diff</td><td>Certified Asterisk 11.6</td></tr>
<tr><td>http://downloads.asterisk.org/pub/security/AST-2016-002-13.1.diff</td><td>Certified Asterisk 13.1</td></tr>
<tr><td>http://downloads.asterisk.org/pub/security/AST-2016-002-1.8.diff</td><td>Asterisk 1.8</td></tr>
<tr><td>http://downloads.asterisk.org/pub/security/AST-2016-002-11.diff</td><td>Asterisk 11</td></tr>
<tr><td>http://downloads.asterisk.org/pub/security/AST-2016-002-12.diff</td><td>Asterisk 12</td></tr>
<tr><td>http://downloads.asterisk.org/pub/security/AST-2016-002-13.diff</td><td>Asterisk 13</td></tr>
</table>

Links	https://issues.asterisk.org/jira/browse/ASTERISK-25397

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This document may be superseded by later versions; if so, the latest version will be posted at http://downloads.digium.com/pub/security/AST-2016-002.pdf and http://downloads.digium.com/pub/security/AST-2016-002.html

<table>
<tr><th colspan="3">Revision History</th></tr>
<tr><th>Date</th><th>Editor</th><th>Revisions Made</th></tr>
<tr><td>September 29, 2015</td><td>Richard Mudgett</td><td>Initial document created</td></tr>
<tr><td>February 15, 2016</td><td>Kevin Harwell</td><td>CVE assignment</td></tr>
</table>