Product	Asterisk
Summary	Asterisk Susceptibility to POODLE Vulnerability
Nature of Advisory	Unauthorized Data Disclosure
Susceptibility	Remote Unauthenticated Sessions
Severity	Medium
Exploits Known	No
Reported On	16 October 2014
Reported By	abelbeck
Posted On	20 October 2014
Last Updated On	October 20, 2014
Advisory Contact	Matt Jordan <mjordan AT digium DOT com>
CVE Name	CVE-2014-3566

Description	The POODLE vulnerability – described under CVE-2014-3566 – is described at https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3566. This advisory describes the Asterisk's project susceptibility to this vulnerability. The POODLE vulnerability consists of two issues: 1) A vulnerability in the SSL protocol version 3.0. This vulnerability has no known solution. 2) The ability to force a fallback to SSLv3 when a TLS connection is negotiated. Asterisk is susceptible to both portions of the vulnerability in different places. 1) The res_jabber and res_xmpp module both use SSLv3 exclusively, and are hence susceptible to POODLE. 2) The core TLS handling, used by the chan_sip channel driver, Asterisk Manager Interface (AMI), and the Asterisk HTTP server, defaults to allowing SSLv3/SSLv2 fallback. This allows a MITM to potentially force a connection to fallback to SSLv3, exposing it to the POODLE vulnerability.

Resolution	Asterisk has been patched such that it no longer uses SSLv3 for the res_jabber/res_xmpp modules. Additionally, when the encryption method is not specified, the default handling in the TLS core no longer allows for a fallback to SSLv3 or SSLv2. 1) Users of Asterisk's res_jabber or res_xmpp modules should upgrade to the versions of Asterisk specified in this advisory. 2) Users of Asterisk's chan_sip channel driver, AMI, and HTTP server may set the “tlsclientmethod” or “sslclientmethod” to “tlsv1” to force TLSv1 as the only

	allowed encryption method. Alternatively, they may also upgrade to the versions of Asterisk specified in this advisory. Users of Asterisk are encouraged to NOT specify “sslv2” or “sslv3”. Doing so will now emit a WARNING.

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
Certified Asterisk	1.8.28	All versions
Certified Asterisk	11.6	All versions

Corrected In	
Product	**Release**
Asterisk Open Source	1.8.31.1, 11.13.1, 12.6.1
Certified Asterisk	1.8.28-cert2, 11.6-cert7

Patches	
SVN URL	**Revision**
http://downloads.asterisk.org/pub/security/AST-2014-011-1.8.diff	Asterisk 1.8
http://downloads.asterisk.org/pub/security/AST-2014-011-11.diff	Asterisk 11
http://downloads.asterisk.org/pub/security/AST-2014-011-12.diff	Asterisk 12
http://downloads.asterisk.org/pub/security/AST-2014-011-1.8.28.diff	Certified Asterisk 1.8.28
http://downloads.asterisk.org/pub/security/AST-2014-011-11.6.diff	Certified Asterisk 11.6

Links	https://issues.asterisk.org/jira/browse/ASTERISK-24425

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-2014-011.pdf and http://downloads.digium.com/pub/security/AST-2014-011.html

Revision History		
Date	**Editor**	**Revisions Made**
October 19	Matt Jordan	Initial Revision