Product	Asterisk
Summary	Remote crash when handling out of call message in certain dialplan configurations
Nature of Advisory	Remotely triggered crash of Asterisk
Susceptibility	Remote authenticated sessions
Severity	Minor
Exploits Known	No
Reported On	05 September 2014
Reported By	Philippe Lindheimer
Posted On	18 September 2014
Last Updated On	September 18, 2014
Advisory Contact	Matt Jordan <mjordan AT digium DOT com>
CVE Name	CVE-2014-6610

Description	When an out of call message – delivered by either the SIP or PJSIP channel driver or the XMPP stack - is handled in Asterisk, a crash can occur if the channel servicing the message is sent into the ReceiveFax dialplan application while using the res_fax_spandsp module. Note that this crash does not occur when using the res_fax_digium module. While this crash technically occurs due to a configuration issue, as attempting to receive a fax from a channel driver that only contains textual information will never succeed, the likelihood of having it occur is sufficiently high as to warrant this advisory.

Resolution	The fax family of applications have been updated to handle the Message channel driver correctly. Users using the fax family of applications along with the out of call text messaging features are encouraged to upgrade their versions of Asterisk to the versions specified in this security advisory. Additionally, users of Asterisk are encouraged to use a separate dialplan context to process text messages. This avoids issues where the Message channel driver is passed to dialplan applications that assume a media stream is available. Note that the various channel drivers and stacks provide such an option; an example being the SIP channel driver's outofcall_message_context option.

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

Corrected In	
Product	**Release**
Asterisk Open Source	11.12.1, 12.5.1
Certified Asterisk	11.6-cert6

Patches	
SVN URL	**Revision**
http://downloads.asterisk.org/pub/security/AST-2014-010-11.diff	Asterisk 11
http://downloads.asterisk.org/pub/security/AST-2014-010-12.diff	Asterisk 12
http://downloads.asterisk.org/pub/security/AST-2014-010-11.6.diff	Certified Asterisk 11.6

Links	https://issues.asterisk.org/jira/browse/ASTERISK-24301

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This document may be superseded by later versions; if so, the latest version will be posted at http://downloads.digium.com/pub/security/AST-2014-010.pdf and http://downloads.digium.com/pub/security/AST-2014-010.html

Revision History		
Date	**Editor**	**Revisions Made**
18 September, 2014	Matt Jordan	Initial Draft
18 September, 2014	Matt Jordan	Added CVE