Asterisk Project Security Advisory - AST-2016-003

Product	Asterisk
Summary	Remote crash vulnerability when receiving UDPTL FAX data.
Nature of Advisory	Denial of Service
Susceptibility	Remote Authenticated Sessions
Severity	Minor
Exploits Known	Yes
Reported On	December 2, 2015
Reported By	Walter Dokes, Torrey Searle
Posted On	February 3, 2016
Last Updated On	February 15, 2016
Advisory Contact	Richard Mudgett <rmudgett AT digium DOT com>
CVE Name	CVE-2016-2232

Description	If no UDPTL packets are lost there is no problem. However, a lost packet causes Asterisk to use the available error correcting redundancy packets. If those redundancy packets have zero length then Asterisk uses an uninitialized buffer pointer and length value which can cause invalid memory accesses later when the packet is copied.

Resolution	Upgrade to a released version with the fix incorporated or apply patch.

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

Corrected In	
Product	**Release**
Asterisk Open Source	11.21.1, 13.7.1
Certified Asterisk	11.6-cert12, 13.1-cert3

Patches	
SVN URL	**Revision**
http://downloads.asterisk.org/pub/security/AST-2016-003-1.8.28.diff	Certified Asterisk 1.8.28
http://downloads.asterisk.org/pub/security/AST-2016-003-11.6.diff	Certified Asterisk 11.6
http://downloads.asterisk.org/pub/security/AST-2016-003-13.1.diff	Certified Asterisk 13.1
http://downloads.asterisk.org/pub/security/AST-2016-003-1.8.diff	Asterisk 1.8
http://downloads.asterisk.org/pub/security/AST-2016-003-11.diff	Asterisk 11
http://downloads.asterisk.org/pub/security/AST-2016-003-12.diff	Asterisk 12
http://downloads.asterisk.org/pub/security/AST-2016-003-13.diff	Asterisk 13

Links	https://issues.asterisk.org/jira/browse/ASTERISK-25603

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This document may be superseded by later versions; if so, the latest version will be posted at http://downloads.digium.com/pub/security/AST-2016-003.pdf and http://downloads.digium.com/pub/security/AST-2016-003.html

Revision History		
Date	**Editor**	**Revisions Made**
December 7, 2015	Richard Mudgett	Initial document created
February 15, 2016	Kevin Harwell	CVE assignment