

Asterisk Project Security Advisory - AST-2016-004

Product	Asterisk
Summary	Long Contact URIs in REGISTER requests can crash Asterisk
Nature of Advisory	Remote Crash
Susceptibility	Remote Authenticated Sessions
Severity	Major
Exploits Known	No
Reported On	January 19, 2016
Reported By	George Joseph
Posted On	
Last Updated On	February 10, 2016
Advisory Contact	Mark Michelson <mmichelson AT digium DOT com>
CVE Name	

Description	<p>Asterisk may crash when processing an incoming REGISTER request if that REGISTER contains a Contact header with a lengthy URI.</p> <p>This crash will only happen for requests that pass authentication. Unauthenticated REGISTER requests will not result in a crash occurring.</p> <p>This vulnerability only affects Asterisk when using PJSIP as its SIP stack. The chan_sip module does not have this problem.</p>
--------------------	--

Resolution	Measures have been put in place to ensure that REGISTER requests with long Contact URIs are rejected instead of causing a crash.
-------------------	--

Affected Versions		
Product	Release Series	
Asterisk Open Source	11.x	Unaffected
Asterisk Open Source	13.x	All versions
Certified Asterisk	11.6	Unaffected
Certified Asterisk	13.1	All versions

Asterisk Project Security Advisory - AST-2016-004

Copyright © 2016 Digium, Inc. All Rights Reserved.

Permission is hereby granted to distribute and publish this advisory in its original, unaltered form.

Asterisk Project Security Advisory - AST-2016-004

Corrected In	
Product	Release
Asterisk Open Source	13.8.1
Certified Asterisk	13.1-cert5

Patches	
SVN URL	Revision

Links

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This document may be superseded by later versions; if so, the latest version will be posted at 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-2016-004.pdf> and <http://downloads.digium.com/pub/security/AST-2016-004.html>

Revision History		
Date	Editor	Revisions Made
February 10, 2016	Mark Michelson	Initial creation

Asterisk Project Security Advisory - AST-2016-004

Copyright © 2016 Digium, Inc. All Rights Reserved.

Permission is hereby granted to distribute and publish this advisory in its original, unaltered form.