

Asterisk Project Security Advisory - AST-2014-004

Product	Asterisk
Summary	Remote Crash Vulnerability in PJSIP Channel Driver Subscription Handling
Nature of Advisory	Denial of Service
Susceptibility	Remote Authenticated Sessions
Severity	Moderate
Exploits Known	No
Reported On	January 14th, 2014
Reported By	Mark Michelson
Posted On	March 10, 2014
Last Updated On	March 10, 2014
Advisory Contact	Matt Jordan <mjordan AT digium DOT com>
CVE Name	CVE-2014-2289

Description	A remotely exploitable crash vulnerability exists in the PJSIP channel driver's handling of SUBSCRIBE requests. If a SUBSCRIBE request is received for the presence Event, and that request has no Accept headers, Asterisk will attempt to access an invalid pointer to the header location. Note that this issue was fixed during a re-architecture of the res_pjsip_pubsub module in Asterisk 12.1.0. As such, this issue has already been resolved in a released version of Asterisk. This notification is being released for users of Asterisk 12.0.0.
--------------------	---

Resolution	Upgrade to Asterisk 12.1.0, or apply the patch noted below to Asterisk 12.0.0.
-------------------	--

Affected Versions		
Product	Release Series	
Asterisk Open Source	12.x	12.0.0

Corrected In	
Product	Release
Asterisk Open Source	12.1.0

Asterisk Project Security Advisory - AST-2014-004

Copyright © 2014 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-2014-004

Patches	
SVN URL	Revision
http://downloads.asterisk.org/pub/security/AST-2014-004-12.diff	Asterisk 12

Links	https://issues.asterisk.org/jira/browse/ASTERISK-23139
--------------	---

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This document may be superseded by later versions; if so, the latest version will be posted at 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-2014-004.pdf> and <http://downloads.digium.com/pub/security/AST-2014-004.html>

Revision History		
Date	Editor	Revisions Made
03/05/14	Matt Jordan	Initial Revision

Asterisk Project Security Advisory - AST-2014-004

Copyright © 2014 Digium, Inc. All Rights Reserved.

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