Product	Asterisk
Summary	Username disclosure in SIP channel driver
Nature of Advisory	Unauthorized data disclosure
Susceptibility	Remote Unauthenticated Sessions
Severity	Moderate
Exploits Known	No
Reported On	January 30, 2013
Reported By	Walter Doekes, OSSO B.V.
Posted On	February 21, 2013
Last Updated On	March 27, 2013
Advisory Contact	Kinsey Moore <kmoore@digium.com>
CVE Name	CVE-2013-2264

Description	When authenticating via SIP with alwaysauthreject enabled, allowguest disabled, and autocreatepeer disabled, Asterisk discloses whether a user exists for INVITE, SUBSCRIBE, and REGISTER transactions in multiple ways. This information was disclosed: * when a “407 Proxy Authentication Required” response was sent instead of “401 Unauthorized” response. * due to the presence or absence of additional tags at the end of “403 Forbidden” such as “(Bad auth)”. * when a “401 Unauthorized” response was sent instead of “403 Forbidden” response after a retransmission. * when retransmissions were sent when a matching peer did not exist, but were not when a matching peer did exist.

Resolution	This issue can only be mitigated by upgrading to versions of Asterisk that contain the patch or applying the patch.

Affected Versions		
Product	**Release Series**	
Asterisk Open Source	1.8.x	All Versions
Asterisk Open Source	10.x	All Versions
Asterisk Open Source	11.x	All Versions
Certified Asterisk	1.8.15	All Versions
Asterisk Business Edition	C.3.x	All Versions
Asterisk Digiumphones	10.x-digiumphones	All Versions

Corrected In	
Product	**Release**
Asterisk Open Source	1.8.20.2, 10.12.2, 11.2.2
Asterisk Digiumphones	10.12.2-digiumphones
Certified Asterisk	1.8.15-cert2
Asterisk Business Edition	C.3.8.1

Patches	
SVN URL	**Revision**
http://downloads.asterisk.org/pub/security/AST-2013-003-1.8.diff	Asterisk 1.8
http://downloads.asterisk.org/pub/security/AST-2013-003-10.diff	Asterisk 10
http://downloads.asterisk.org/pub/security/AST-2013-003-11.diff	Asterisk 11
http://downloads.asterisk.org/pub/security/AST-2013-003-1.8.15-cert.diff	Certified Asterisk 1.8.15
http://downloads.asterisk.org/pub/security/AST-2013-003-C.3.diff	Asterisk BE C.3

Links	https://issues.asterisk.org/jira/browse/ASTERISK-21013

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This document may be superseded by later versions; if so, the latest version will be posted at http://downloads.digium.com/pub/security/AST-2013-003.pdf and http://downloads.digium.com/pub/security/AST-2013-003.html

Revision History		
Date	**Editor**	**Revisions Made**
2013-02-20	Kinsey Moore	Initial revision.
2013-02-27	Kinsey Moore	Added Asterisk BE patch information.
2013-02-27	Kinsey Moore	Corrected open source Asterisk versions.