Product	Asterisk
Summary	PJSIP ACLs are not loaded on startup
Nature of Advisory	Unauthorized Access
Susceptibility	Remote unauthenticated sessions
Severity	Moderate
Exploits Known	No
Reported On	28 October, 2014
Reported By	Jonathan Rose
Posted On	20 November, 2014
Last Updated On	November 21, 2014
Advisory Contact	Jonathan Rose <jrose AT digium DOT com>
CVE Name	CVE-2014-8413

Description	The Asterisk module res_pjsip_acl provides the ability to configure ACLs that may be used to reject SIP requests from various hosts. In affected versions of Asterisk, this module fails to create and apply ACLs defined in pjsip.conf. This may be worked around by reloading res_pjsip manually after res_pjsip_acl is loaded.

Resolution	The PJSIP ACL code has been changed to create and apply the ACLs properly at startup.

Affected Versions		
Product	**Release Series**	
Asterisk Open Source	12.x	All versions
Asterisk Open Source	13.x	All versions

Corrected In	
Product	**Release**
Asterisk Open Source	12.7.1, 13.0.1

Patches

SVN URL	Revision
http://downloads.asterisk.org/pub/security/ AST-2014-013-12.diff	Asterisk 12
http://downloads.asterisk.org/pub/security/ AST-2014-013-13.diff	Asterisk 13

Links	https://issues.asterisk.org/jira/browse/ASTERISK-24531

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This document may be superseded by later versions; if so, the latest version will be posted at http://downloads.digium.com/pub/security/AST-2014-013.pdf and http://downloads.digium.com/pub/security/AST-2014-013.html

Revision History

Date	Editor	Revisions Made
17 November, 2014	Jonathan Rose	Initial Advisory created