Product	Asterisk
Summary	PJSIP endpoint presence disclosure when using ACL
Nature of Advisory	Unauthorized data disclosure
Susceptibility	Remote Unauthenticated Sessions
Severity	Minor
Exploits Known	No
Reported On	April 19, 2018
Reported By	John
Posted On	June 11, 2018
Last Updated On	June 12, 2018
Advisory Contact	Rmudgett AT digium DOT com
CVE Name	CVE-2018-12227

Description	When endpoint specific ACL rules block a SIP request they respond with a 403 forbidden. However, if an endpoint is not identified then a 401 unauthorized response is sent. This vulnerability just discloses which requests hit a defined endpoint. The ACL rules cannot be bypassed to gain access to the disclosed endpoints.

Resolution	Endpoint specific ACL rules now respond with a 401 challenge which is the same as if an endpoint were not identified. An alternate is to use global ACL rules to avoid the information disclosure.

Affected Versions		
Product	**Release Series**	
Asterisk Open Source	13.x	13.10.0 and later
Asterisk Open Source	14.x	All releases
Asterisk Open Source	15.x	All releases
Certified Asterisk	13.18	All releases
Certified Asterisk	13.21	All releases

Corrected In	
Product	**Release**
Asterisk Open Source	13.21.1, 14.7.7, 15.4.1
Certified Asterisk	13.18-cert4, 13.21-cert2

Patches	
SVN URL	**Revision**
http://downloads.asterisk.org/pub/security/AST-2018-008-13.diff	Asterisk 13
http://downloads.asterisk.org/pub/security/AST-2018-008-14.diff	Asterisk 14
http://downloads.asterisk.org/pub/security/AST-2018-008-15.diff	Asterisk 15
http://downloads.asterisk.org/pub/security/AST-2018-008-13.18.diff	Certified Asterisk 13.18
http://downloads.asterisk.org/pub/security/AST-2018-008-13.21.diff	Certified Asterisk 13.21

Links	https://issues.asterisk.org/jira/browse/ASTERISK-27818

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This document may be superseded by later versions; if so, the latest version will be posted at http://downloads.digium.com/pub/security/AST-2018-008.pdf and http://downloads.digium.com/pub/security/AST-2018-008.html

Revision History		
Date	**Editor**	**Revisions Made**
May 1, 2018	Richard Mudgett	Initial revision
June 11, 2018	Richard Mudgett	Added Certified Asterisk 13.21

June 12, 2018	Kevin Harwell	Added CVE and issue link