Product	Asterisk
Summary	TLS Certificate Common name NULL byte exploit
Nature of Advisory	Man in the Middle Attack
Susceptibility	Remote Authenticated Sessions
Severity	Major
Exploits Known	None
Reported On	12 January, 2015
Reported By	Maciej Szmigiero
Posted On	March 04, 2015
Last Updated On	
Advisory Contact	Jonathan Rose <jrose AT digium DOT com>
CVE Name	CVE-2015-3008

Description	When Asterisk registers to a SIP TLS device and and verifies the server, Asterisk will accept signed certificates that match a common name other than the one Asterisk is expecting if the signed certificate has a common name containing a null byte after the portion of the common name that Asterisk expected. For example, if Asterisk is trying to register to www.domain.com, Asterisk will accept certificates of the form www.domain.com\x00www.someotherdomain.com – for more information on this exploit, see https://fotisl.com/blog/2009/10/the-null-certificate-prefix-bug/

Resolution	Asterisk has been patched to verify that the common name length of the certificate matches the common name that Asterisk actually reads. Asterisk will not accept certificates with common names that contain null bytes.

Affected Versions		
Product	**Release Series**	
Asterisk Open Source	1.8.x	All versions
Asterisk Open Source	11.x	All versions
Asterisk Open Source	12.x	All versions
Asterisk Open Source	13.x	All versions
Certified Asterisk	1.8.28	All versions
Certified Asterisk	11.6	All versions
Certified Asterisk	13.1	All versions

Corrected In	
Product	**Release**
Asterisk Open Source	1.8.32.3, 11.17.1, 12.8.2 13.3.2
Certified Asterisk	1.8.28-cert5, 11.6-cert11, 13.1-cert2

Patches	
SVN URL	**Revision**
http://downloads.asterisk.org/pub/security/AST-2015-003-1.8.28.diff	Certified Asterisk 1.8.28
http://downloads.asterisk.org/pub/security/AST-2015-003-11.6.diff	Certified Asterisk 11.6
http://downloads.asterisk.org/pub/security/AST-2015-003-13.1.diff	Certified Asterisk 13.1
http://downloads.asterisk.org/pub/security/AST-2015-003-1.8.diff	Asterisk 1.8
http://downloads.asterisk.org/pub/security/AST-2015-003-11.diff	Asterisk 11
http://downloads.asterisk.org/pub/security/AST-2015-003-12.diff	Asterisk 12
http://downloads.asterisk.org/pub/security/AST-2015-003-13.diff	Asterisk 13

Links	https://issues.asterisk.org/jira/browse/ASTERISK-24847

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This document may be superseded by later versions; if so, the latest version will be posted at http://downloads.digium.com/pub/security/AST-2015-003.pdf and http://downloads.digium.com/pub/security/AST-2015-003.html

Revision History		
Date	**Editor**	**Revisions Made**
19 March, 2015	Jonathan Rose	Initial creation of document
08 April, 2015	Matt Jordan	Added CVE.