Product	Asterisk
Summary	Denial of Service Through Exploitation of Device State Caching
Nature of Advisory	Denial of Service
Susceptibility	Remote Unauthenticated Sessions
Severity	Critical
Exploits Known	None
Reported On	26 July, 2012
Reported By	Russell Bryant
Posted On	2 January, 2013
Last Updated On	January 3, 2013
Advisory Contact	Matt Jordan <mjordan AT digium DOT com>
CVE Name	CVE-2012-5977

Description	Asterisk maintains an internal cache for devices. The device state cache holds the state of each device known to Asterisk, such that consumers of device state information can query for the last known state for a particular device, even if it is not part of an active call. The concept of a device in Asterisk can include things that do not have a physical representation. One way that this currently occurs is when anonymous calls are allowed in Asterisk. A device is automatically created and stored in the cache for each anonymous call that occurs; this is possible in the SIP and IAX2 channel drivers and through channel drivers that utilize the res_jabber/res_xmpp resource modules (Gtalk, Jingle, and Motif). Attackers exploiting this vulnerability can attack an Asterisk system configured to allow anonymous calls by varying the source of the anonymous call, continually adding devices to the device state cache and consuming a system's resources.

Resolution	Channels that are not associated with a physical device are no longer stored in the device state cache. This affects Local, DAHDI, SIP and IAX2 channels, and any channel drivers built on the res_jabber/res_xmpp resource modules (Gtalk, Jingle, and Motif).

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	1.8.11	All Versions
Asterisk Digiumphones	10.x-digiumphones	All Versions

Corrected In

Product	Release
Asterisk Open Source	1.8.19.1, 10.11.1, 11.1.2
Certified Asterisk	1.8.11-cert10
Asterisk Digiumphones	10.11.1-digiumphones

Patches

SVN URL	Revision
http://downloads.asterisk.org/pub/security/AST-2012-015-1.8.diff	Asterisk 1.8
http://downloads.asterisk.org/pub/security/AST-2012-015-10.diff	Asterisk 10
http://downloads.asterisk.org/pub/security/AST-2012-015-11.diff	Asterisk 11

Links	https://issues.asterisk.org/jira/browse/ASTERISK-20175

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This document may be superseded by later versions; if so, the latest version will be posted at http://downloads.digium.com/pub/security/AST-2012-015.pdf and http://downloads.digium.com/pub/security/AST-2012-015.html

Revision History

Date	Editor	Revisions Made

19 November 2012	Matt Jordan	Initial Draft
03 January 2013	Matt Jordan	Updated Asterisk 11 version