Asterisk Project Security Advisory - AST-2016-005

Product	Asterisk
Summary	TCP denial of service in PJProject
Nature of Advisory	Crash/Denial of Service
Susceptibility	Remote Unauthenticated Sessions
Severity	Critical
Exploits Known	No
Reported On	February 15, 2016
Reported By	George Joseph
Posted On	
Last Updated On	March 3, 2016
Advisory Contact	Mark Michelson <mark DOT michelson AT digium DOT com>
CVE Name	

Description	PJProject has a limit on the number of TCP connections that it can accept. Furthermore, PJProject does not close TCP connections it accepts. By default, this value is approximately 60. An attacker can deplete the number of allowed TCP connections by opening TCP connections and sending no data to Asterisk. If PJProject has been compiled in debug mode, then once the number of allowed TCP connections has been depleted, the next attempted TCP connection to Asterisk will crash due to an assertion in PJProject. If PJProject has not been compiled in debug mode, then any further TCP connection attempts will be rejected. This makes Asterisk unable to process TCP SIP traffic. Note that this only affects TCP/TLS, since UDP is connectionless. Also note that this does not affect chan_sip.

Resolution	PJProject has a compile-time constant that controls the maximum number of TCP connections that can be handled. Those who compile PJProject on their own are encouraged to set this to a value that is more amenable to the number of TCP connections that Asterisk should be able to handle. In PJProject's pjlib/include/pj/config_site.h, add the following prior to compiling PJProject: # define PJ_IOQUEUE_MAX_HANDLES (FD_SETSIZE)

	This is part of a larger set of recommended definitions to place in config_site.h of PJProject. See the Asterisk “Building and Installing PJProject” wiki page for other recommended settings. Packagers of PJProject have updated their packages to have these constants defined, so if your package is kept up to date, you should already be fine. In addition, the Asterisk project has recently been modified to be able to perform a static build of PJProject. By running the Asterisk configure script with the --with-pjproject-bundled option, the latest PJProject will be downloaded and installed, and the compile-time constants will be set to appropriate values. Asterisk has also been updated to monitor incoming TCP connections. If a TCP connection is opened and no SIP request is received on that connection within a certain amount of time, then Asterisk will shut down the connection.

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

Corrected In	
Product	**Release**
Asterisk Open Source	13.8.1
Certified Asterisk	13.1-cert5

Patches	
SVN URL	**Revision**

Links	

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-2016-005.pdf and http://downloads.digium.com/pub/security/AST-2016-005.html

Revision History		
Date	**Editor**	**Revisions Made**