Product	Asterisk
Summary	Crashes due to large stack allocations when using TCP
Nature of Advisory	Stack Overflow
Susceptibility	Remote Unauthenticated Sessions (SIP, HTTP) Remote Authenticated Sessions (XMPP)
Severity	Critical
Exploits Known	No
Reported On	7 November, 2012
Reported By	Walter Doekes, Brandon Edwards of Exodus Intelligence
Posted On	2 January, 2013
Last Updated On	January 7, 2013
Advisory Contact	Mark Michelson <mmichelson AT digium DOT com>
CVE Name	CVE-2012-5976

Description	Asterisk has several places where messages received over various network transports may be copied in a single stack allocation. In the case of TCP, since multiple packets in a stream may be concatenated together, this can lead to large allocations that overflow the stack. In the case of SIP and HTTP, it is possible to do this before a session is established. Keep in mind that SIP over UDP is not affected by this vulnerability. With XMPP, a session must first be established before the vulnerability may be exploited. The XMPP vulnerability exists both in the res_jabber.so module in Asterisk 1.8, 10, and 11 as well as the res_xmpp.so module in Asterisk 11.

Resolution	Stack allocations when using TCP have either been eliminated in favor of heap allocations or have had an upper bound placed on them to ensure that the stack will not overflow. For SIP, the allocation now has an upper limit. For HTTP, the allocation is now a heap allocation instead of a stack allocation. For XMPP, the allocation has been eliminated since it was unnecessary.

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	SIP: unaffected HTTP and XMPP: 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-2012-014-1.8.diff`	Asterisk 1.8
`http://downloads.asterisk.org/pub/security/AST-2012-014-10.diff`	Asterisk 10
`http://downloads.asterisk.org/pub/security/AST-2012-014-11.diff`	Asterisk 11

Links	https://issues.asterisk.org/jira/browse/ASTERISK-20658

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This document may be superseded by later versions; if so, the latest version will be posted at http://downloads.digium.com/pub/security/AST-2012-014.pdf and http://downloads.digium.com/pub/security/AST-2012-014.html

Revision History		
Date	**Editor**	**Revisions Made**
19 November, 2012	Mark Michelson	Initial Draft

02 January, 2013	Matt Jordan	Removed ABE from affected products
02 January, 2013	Matt Jordan	Updated advisory to note that HTTP can be exploited before authentication
03 January, 2013	Matt Jordan	Updated Asterisk 11 version
07 January, 2013	Matt Jordan	Updated with Brandon Edwards of Exodus Intelligence, who independently discovered the HTTP vulnerability