Product	Asterisk
Summary	Stack Buffer Overflow in HTTP Manager
Nature of Advisory	Exploitable Stack Buffer Overflow
Susceptibility	Remote Unauthenticated Sessions
Severity	Critical
Exploits Known	No
Reported On	03/15/2012
Reported By	Russell Bryant
Posted On	03/15/2012
Last Updated On	March 15, 2012
Advisory Contact	Matt Jordan < mjordan AT digium DOT com >
CVE Name	

Description	An attacker attempting to connect to an HTTP session of the Asterisk Manager Interface can send an arbitrarily long string value for HTTP Digest Authentication. This causes a stack buffer overflow, with the possibility of remote code injection.

Resolution	Upgrade to one of the versions of Asterisk listed in the “Corrected In” section, or apply a patch specified in the “Patches” section.

Affected Versions		
Product	**Release Series**	
Asterisk Open Source	1.8.x	All versions
Asterisk Open Source	10.x	All versions

Corrected In	
Product	**Release**
Asterisk Open Source	1.8.10.1
Asterisk Open Source	10.2.1

Patches	
SVN URL	**Revision**

http://downloads.asterisk.org/pub/security/AST-2012-003-1.8.diff	v1.8
http://downloads.asterisk.org/pub/security/AST-2012-003-10.diff	v10

Links	https://issues.asterisk.org/jira/browse/ASTERISK-19542

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This document may be superseded by later versions; if so, the latest version will be posted at http://downloads.digium.com/pub/security/AST-2012-003.pdf and http://downloads.digium.com/pub/security/AST-2012-003.html

Revision History		
Date	**Editor**	**Revisions Made**
03-15-2012	Matt Jordan	Initial release
03-16-2012	Matt Jordan	Corrected links