Asterisk Project Security Advisory - AST-2008-004

Product	Asterisk
Summary	Format String Vulnerability in Logger and Manager
Nature of Advisory	Denial of Service
Susceptibility	Remote Unauthenticated Sessions
Severity	Moderate
Exploits Known	No
Reported On	March 13, 2008
Reported By	Steve Davies (bugs.digium.com user stevedavies) Brandon Kruse (bugs.digium.com user bkruse)
Posted On	March 18, 2008
Last Updated On	December 15, 2008
Advisory Contact	Joshua Colp <jcolp@digium.com>
CVE Name	CVE-2008-1333

Description	Logging messages displayed using the ast_verbose logging API call are not displayed as a character string, they are displayed as a format string. Output as a result of the Manager command “command” is not appended to the resulting response message as a character string, it is appended as a format string. It is possible in both instances for an attacker to provide a formatted string as a value for input which can cause a crash.

Resolution	Input given to both the ast_verbose logging API call and astman_append function is now interpreted as a character string and not as a format string.

Affected Versions		
Product	**Release Series**	
Asterisk Open Source	1.0.x	Unaffected
Asterisk Open Source	1.2.x	Unaffected
Asterisk Open Source	1.4.x	Unaffected
Asterisk Open Source	1.6.x	All versions prior to 1.6.0-beta6
Asterisk Business Edition	A.x.x	Unaffected
Asterisk Business Edition	B.x.x	Unaffected
Asterisk Business Edition	C.x.x	Unaffected
AsteriskNOW	1.0.x	Unaffected
Asterisk Appliance Developer Kit	0.x.x	Unaffected
s800i (Asterisk Appliance)	1.0.x	Unaffected

Corrected In	
Product	**Release**
Asterisk Open Source	1.6.0-beta6, available from http://downloads.digium.com/pub/telephony/asterisk

Patches	
URL	**Version**
http://downloads.digium.com/pub/security/AST-2008-004-1.6.0.patch	1.6.0

Links	http://bugs.digium.com/view.php?id=12205 http://bugs.digium.com/view.php?id=12206

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This document may be superseded by later versions; if so, the latest version will be posted at http://downloads.digium.com/pub/security/AST-2008-004.pdf and http://downloads.digium.com/pub/security/AST-2008-004.html

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

2008-03-18	Joshua Colp	Initial Release
2008-12-15	Joshua Colp	Add Patches