Product	Asterisk
Summary	Dialplan injection vulnerability
Nature of Advisory	Data injection vulnerability
Susceptibility	Remote Unauthenticated Sessions
Severity	Critical
Exploits Known	Yes
Reported On	10/02/10
Reported By	Hans Petter Selasky
Posted On	16/02/10
Last Updated On	February 25, 2010
Advisory Contact	Leif Madsen < lmadsen AT digium DOT com >
CVE Name	CVE-2010-0685

Description	A common usage of the ${EXTEN} channel variable in a dialplan with wildcard pattern matches can lead to a possible string injection vulnerability. By having a wildcard match in a dialplan, it is possible to allow unintended calls to be executed, such as in this example: exten => _X.,1,Dial(SIP/${EXTEN}) If you have a channel technology which can accept characters other than numbers and letters (such as SIP) it may be possible to craft an INVITE which sends data such as 300&Zap/g1/4165551212 which would create an additional outgoing channel leg that was not originally intentioned by the dialplan programmer. Usage of the wildcard character is common in dialplans that require variable number length, such as European dial strings. Please note that this is not limited to an specific protocol or the Dial() application. The expansion of variables into programmatically-interpreted strings is a common behavior in many script or script-like languages, Asterisk included. The ability for a variable to directly replace components of a command is a feature, not a bug - that is the entire point of string expansion. However, it is often the case due to expediency or design misunderstanding that a developer will not examine and filter string data from external sources before passing it into potentially harmful areas of their dialplan. With the flexibility of the design of Asterisk come these risks if the dialplan designer is not suitably cautious as to how foreign data is allowed to continue into the system.

	This security release is intended to raise awareness of how it is possible to insert malicious strings into dialplans, and to advise developers to read the best practices documents so that they may easily avoid these dangers.

Resolution	One resolution is to wrap the ${EXTEN} channel variable with the FILTER() dialplan function to only accept characters which are expected by the dialplan programmer. The recommendation is for this to be the first priority in all contexts defined as incoming contexts in the channel driver configuration files. Examples of this and other best practices can be found in the new README-SERIOUSLY.bestpractices.txt document in the top level folder of your Asterisk sources. Asterisk 1.2.40 has also been released with a backport of the FILTER() dialplan function from 1.4 in order to provide the tools required to resolve this issue in your dialplan.

Affected Versions		
Product	**Release Series**	
Asterisk Open Source	1.2.x	All versions
Asterisk Open Source	1.4.x	All versions
Asterisk Open Source	1.6.x	All versions
Asterisk Business Edition	B.x.x	All versions
Asterisk Business Edition	C.x.x	All versions
Switchvox	None	No versions affected

Document	
SVN URL	**Branch**
http://svn.asterisk.org/svn/asterisk/branches/1.2/README-SERIOUSLY.bestpractices.txt	v1.2
http://svn.asterisk.org/svn/asterisk/branches/1.4/README-SERIOUSLY.bestpractices.txt	v1.4
http://svn.asterisk.org/svn/asterisk/branches/1.6.0/README-SERIOUSLY.bestpractices.txt	v1.6.0
http://svn.asterisk.org/svn/asterisk/branches/1.6.1/README-SERIOUSLY.bestpractices.txt	v1.6.1

http://svn.asterisk.org/svn/asterisk/branches/1.6.2/README-SERIOUSLY.bestpractices.txt	v1.6.2

Corrected In	
Product	**Release**
Open Source Asterisk	1.2.40

Links	https://issues.asterisk.org/view.php?id=16810 https://issues.asterisk.org/view.php?id=16808

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-2010-002.pdf and http://downloads.digium.com/pub/security/AST-2010-002.html

Revision History		
Date	**Editor**	**Revisions Made**
16/02/10	Leif Madsen	Initial release
25/02/10	Leif Madsen	Update CVE Name field