Product	Asterisk
Summary	Asterisk installations using cryptographic keys generated by Debian-based systems may be using a vulnerable implementation of OpenSSL
Nature of Advisory	Compromised cryptographic keys
Susceptibility	Users of RSA for IAX2 authentication and users of DUNDi
Severity	Critical
Exploits Known	None specific to Asterisk, but OpenSSL exploits are circulating
Reported On	13 May 2008
Reported By	Luciano Bello
Posted On	May 16, 2008
Last Updated On	May 22, 2008
Advisory Contact	Mark Michelson < mmichelson AT digium DOT com >
CVE Name	CVE-2008-0166

Description	The Debian team recently announced that cryptographic keys generated by their OpenSSL package were created using a random number generator with predictable results. This affects Debian's stable and unstable distributions, as well as Debian-derived systems such as Ubuntu. See the links in the “Links” session of this advisory for more information about the vulnerability. Asterisk is not directly affected by this vulnerability; however, Asterisk's 'astgenkey' script uses OpenSSL in order to generate cryptographic keys. Therefore, Asterisk users who use RSA for authentication of IAX2 calls and who use DUNDi may be using compromised keys. This vulnerability affects any such installation whose cryptographic keys were generated on a Debian-based system, even if the Asterisk installation itself is not on a Debian-based system.

Resolution	Since this is not a vulnerability in Asterisk itself but in a tool that Asterisk uses, there will be no new releases made; however, users who are affected by the Debian OpenSSL vulnerability are strongly encouraged to upgrade their package of OpenSSL to an uncompromised version (version 0.9.8c-4 or later) and regenerate all keys used by Asterisk.

Affected Versions		
Product	**Release Series**	
Asterisk Open Source	1.0.x	N/A
Asterisk Open Source	1.2.x	N/A
Asterisk Open Source	1.4.x	N/A
Asterisk Business Edition	A.x.x	N/A
Asterisk Business Edition	B.x.x	N/A
Asterisk Business Edition	C.x.x	N/A
AsteriskNOW	pre-release	N/A
Asterisk Appliance Developer Kit	0.x.x	N/A
s800i (Asterisk Appliance)	1.0.x	N/A

Corrected In	
Product	**Release**
N/A	N/A

Links	http://www.debian.org/security/2008/dsa-1571 http://wiki.debian.org/SSLkeys

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This document may be superseded by later versions; if so, the latest version will be posted at http://downloads.digium.com/pub/security/AST-2008-007.pdf and http://downloads.digium.com/pub/security/AST-2008-007.html

Revision History		
Date	**Editor**	**Revisions Made**
May 15, 2008	Mark Michelson	Initial advisory