Product	Asterisk
Summary	Possible remote enumeration of SIP endpoints with differing NAT settings
Nature of Advisory	Unauthorized data disclosure
Susceptibility	Remote unauthenticated sessions
Severity	Minor
Exploits Known	Yes
Reported On	2011-07-18
Reported By	Ben Williams
Posted On	
Last Updated On	December 8, 2011
Advisory Contact	Terry Wilson <twilson@digium.com>
CVE Name	

Description	It is possible to enumerate SIP usernames when the general and user/peer NAT settings differ in whether to respond to the port a request is sent from or the port listed for responses in the Via header. In 1.4 and 1.6.2, this would mean if one setting was nat=yes or nat=route and the other was either nat=no or nat=never. In 1.8 and 10, this would mean when one was nat=force_rport or nat=yes and the other was nat=no or nat=comedia.

Resolution	Handling NAT for SIP over UDP requires the differing behavior introduced by these options. To lessen the frequency of unintended username disclosure, the default NAT setting was changed to always respond to the port from which we received the request—the most commonly used option. Warnings were added on startup to inform administrators of the risks of having a SIP peer configured with a different setting than that of the general setting. The documentation now strongly suggests that peers are no longer configured for NAT individually, but through the global setting in the “general” context. For a discussion of the reasons behind this change and why no general fix is provided, please see the mailing list discussion referenced in the “Links” section below.

Affected Versions		
Product	**Release Series**	
Asterisk Open Source	All	All versions

Corrected In
As this is more of an issue with SIP over UDP in general, there is no fix supplied other than documentation on how to avoid the problem. The default NAT setting has been changed to what we believe the most commonly used setting for the respective version in Asterisk 1.4.43, 1.6.2.21, and 1.8.7.2.

Links	http://lists.digium.com/pipermail/asterisk-dev/2011-November/052191.html

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This document may be superseded by later versions; if so, the latest version will be posted at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-2011-013.pdf and
http://downloads.digium.com/pub/security/AST-2011-013.html

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