

Asterisk Project Security Advisory - AST-2008-008

Product	Asterisk
Summary	Remote Crash Vulnerability in SIP channel driver when run in pedantic mode
Nature of Advisory	Denial of Service
Susceptibility	Remote Unauthenticated Sessions
Severity	Critical
Exploits Known	No
Reported On	May 8, 2008
Reported By	Hooi Ng (bugs.digium.com user hooi)
Posted On	May 8, 2008
Last Updated On	June 3, 2008
Advisory Contact	Joshua Colp <jcolp@digium.com>
CVE Name	CVE-2008-2119

Description	During pedantic SIP processing the From header value is passed to the ast_uri_decode function to be decoded. In two instances it is possible for the code to cause a crash as the From header value is not checked to be non-NULL before being passed to the function.
--------------------	--

Resolution	The From header value is now copied into a buffer before being passed to the ast_uri_decode function if pedantic is enabled and in another instance it is checked to be non-NULL before being passed.
-------------------	---

Asterisk Project Security Advisory - AST-2008-008

Copyright © 2008 Digium, Inc. All Rights Reserved.

Permission is hereby granted to distribute and publish this advisory in its original, unaltered form.

Asterisk Project Security Advisory - AST-2008-008

Affected Versions		
Product	Release Series	
Asterisk Open Source	1.0.x	All versions
Asterisk Open Source	1.2.x	All versions prior to 1.2.29
Asterisk Open Source	1.4.x	Not Affected
Asterisk Business Edition	A.x.x	All versions
Asterisk Business Edition	B.x.x	All versions prior to B.2.5.3
Asterisk Business Edition	C.x.x	Not Affected
AsteriskNOW	1.0.x	Not Affected
Asterisk Appliance Developer Kit	0.x.x	Not Affected
s800i (Asterisk Appliance)	1.0.x	Not Affected

Corrected In	
Product	Release
Asterisk Open Source	1.2.29, available from http://downloads.digium.com/pub/telephony/asterisk
Asterisk Business Edition	B.2.5.3

Links	http://bugs.digium.com/view.php?id=12607
--------------	---

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 This document may be superseded by later versions; if so, the latest version will be posted at 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-2008-008.pdf> and <http://downloads.digium.com/pub/security/AST-2008-008.html>

Revision History		
Date	Editor	Revisions Made
2008-06-03	Joshua Colp	Initial Release

Asterisk Project Security Advisory - AST-2008-008

Copyright © 2008 Digium, Inc. All Rights Reserved.

Permission is hereby granted to distribute and publish this advisory in its original, unaltered form.