

Asterisk Project Security Advisory - AST-2008-003

Product	Asterisk
Summary	Unauthenticated calls allowed from SIP channel driver
Nature of Advisory	Authentication Bypass
Susceptibility	Remote Unauthenticated Sessions
Severity	Major
Exploits Known	No
Reported On	March 12, 2008
Reported By	Jason Parker <jparker@digium.com>
Posted On	March 18, 2008
Last Updated On	March 18, 2008
Advisory Contact	Jason Parker <jparker@digium.com>
CVE Name	CVE-2008-1332

Description	Unauthenticated calls can be made via the SIP channel driver using an invalid From header. This acts similarly to the SIP configuration option 'allowguest=yes', in that calls with a specially crafted From header would be sent to the PBX in the context specified in the general section of sip.conf.
--------------------	---

Resolution	<p>A fix has been added which checks for the option 'allowguest' to be enabled before determining that authentication is not required.</p> <p>As a workaround, modify the context in the general section of sip.conf to point to a non-trusted location (example: a non-existent context, or a context that does nothing but hang up the call).</p>
-------------------	---

Asterisk Project Security Advisory - AST-2008-003

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-2008-003

Affected Versions		
Product	Release Series	
Asterisk Open Source	1.0.x	All versions
Asterisk Open Source	1.2.x	All versions prior to 1.2.27
Asterisk Open Source	1.4.x	All versions prior to 1.4.18.1 and 1.4.19-rc3
Asterisk Business Edition	A.x.x	All versions
Asterisk Business Edition	B.x.x	All versions prior to B.2.5.1
Asterisk Business Edition	C.x.x	All versions prior to C.1.6.2
AsteriskNOW	1.0.x	All versions prior to 1.0.2
Asterisk Appliance Developer Kit	SVN	All versions prior to Asterisk 1.4 revision 109393
s800i (Asterisk Appliance)	1.0.x	All versions prior to 1.1.0.2

Corrected In	
Product	Release
Asterisk Open Source	1.2.27, 1.4.18.1/1.4.19-rc3, available from http://downloads.digium.com/pub/telephony/asterisk
Asterisk Business Edition	B.2.5.1, C.1.6.2
AsteriskNOW	1.0.2, available from http://www.asterisknow.org/ Current users can update using the system update feature in the appliance control panel.
Asterisk Appliance Developer Kit	Asterisk 1.4 revision 109393. Available by performing an svn update of the AADK tree.
s800i (Asterisk Appliance)	1.1.0.2

Links

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-2008-003.pdf> and <http://downloads.digium.com/pub/security/AST-2008-003.html>

Asterisk Project Security Advisory - AST-2008-003

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-2008-003

Revision History		
Date	Editor	Revisions Made
2008-03-18	Jason Parker	Initial Release

Asterisk Project Security Advisory - AST-2008-003

Copyright © 2008 Digium, Inc. All Rights Reserved.

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