

Asterisk Project Security Advisory - AST-2011-012

Product	Asterisk
Summary	Remote crash vulnerability in SIP channel driver
Nature of Advisory	Remote crash
Susceptibility	Remote authenticated sessions
Severity	Critical
Exploits Known	No
Reported On	October 4, 2011
Reported By	Ehsan Foroughi
Posted On	October 17, 2011
Last Updated On	October 17, 2011
Advisory Contact	Terry Wilson <twilson@digium.com>
CVE Name	CVE-2011-4063

Description	A remote authenticated user can cause a crash with a malformed request due to an uninitialized variable.
--------------------	--

Resolution	Ensure variables are initialized in all cases when parsing the request.
-------------------	---

Affected Versions		
Product	Release Series	
Asterisk Open Source	1.8.x	All versions
Asterisk Open Source	10.x	All versions (currently in beta)

Corrected In	
Product	Release
Asterisk Open Source	1.8.7.1, 10.0.0-rc1

Patches

Asterisk Project Security Advisory - AST-2011-012

Copyright © 2011 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-2011-012

Download URL	Revision
http://downloads.asterisk.org/pub/security/AST-2011-012-1.8.diff	1.8
http://downloads.asterisk.org/pub/security/AST-2011-012-10.diff	10

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This document may be superseded by later versions; if so, the latest version will be posted at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-2011-012.pdf> and
<http://downloads.digium.com/pub/security/AST-2011-012.html>

Revision History		
Date	Editor	Revisions Made

Asterisk Project Security Advisory - AST-2011-012

Copyright © 2011 Digium, Inc. All Rights Reserved.

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