Product	Asterisk
Summary	IAX2 Call Number Resource Exhaustion
Nature of Advisory	Denial of Service
Susceptibility	Remote unauthenticated sessions
Severity	Major
Exploits Known	Yes - Published by Blake Cornell < blake AT remoteorigin DOT com > on voip0day.com
Reported On	June 22, 2008
Reported By	Noam Rathaus < noamr AT beyondsecurity DOT com >, with his SSD program, also by Blake Cornell
Posted On	September 3, 2009
Last Updated On	September 3, 2009
Advisory Contact	Russell Bryant < russell AT digium DOT com >
CVE Name	CVE-2009-2346

Description	The IAX2 protocol uses a call number to associate messages with the call that they belong to. However, the protocol defines the call number field in messages as a fixed size 15 bit field. So, if all call numbers are in use, no additional sessions can be handled. A call number gets created at the start of an IAX2 message exchange. So, an attacker can send a large number of messages and consume the call number space. The attack is also possible using spoofed source IP addresses as no handshake is required before a call number is assigned.

Resolution	Upgrade to a version of Asterisk listed in this document as containing the IAX2 protocol security enhancements. In addition to upgrading, administrators should consult the users guide section of the IAX2 Security document (IAX2-security.pdf), as well as the sample configuration file for chan_iax2 that have been distributed with those releases for assistance with new options that have been provided.

Discussion	A lot of time was spent trying to come up with a way to resolve this issue in a way that was completely backwards compatible. However, the final resolution ended up requiring a modification to the IAX2 protocol. This modification is referred to as call token validation. Call token validation is used as a handshake before call numbers are assigned to IAX2 connections. Call token validation by itself does not resolve the issue. However, it does allow an IAX2 server to validate that the source of the messages has not been spoofed.

	In addition to call token validation, Asterisk now also has the ability to limit the amount of call numbers assigned to a given remote IP address. The combination of call token validation and call number allocation limits is used to mitigate this denial of service issue. An alternative approach to securing IAX2 would be to use a security layer on top of IAX2, such as DTLS [RFC4347] or IPsec [RFC4301].

Affected Versions

Product	Release Series	
Asterisk Open Source	1.2.x	All versions
Asterisk Open Source	1.4.x	All versions
Asterisk Open Source	1.6.x	All versions
Asterisk Business Edition	B.x.x	All versions
Asterisk Business Edition	C.x.x	All versions
s800i (Asterisk Appliance)	1.3.x	All versions

Corrected In

Product	Release
Asterisk Open Source	1.2.35
Asterisk Open Source	1.4.26.2
Asterisk Open Source	1.6.0.15
Asterisk Open Source	1.6.1.6
Asterisk Business Edition	B.2.5.10
Asterisk Business Edition	C.2.4.3
Asterisk Business Edition	C.3.1.1
S800i (Asterisk Appliance)	1.3.0.3

Patches

Link	Branch
http://downloads.asterisk.org/pub/security/AST-2009-006-1.2.diff.txt	1.2
http://downloads.asterisk.org/pub/security/AST-2009-006-1.4.diff.txt	1.4
http://downloads.asterisk.org/pub/security/AST-2009-006-1.6.0.diff.txt	1.6.0

http://downloads.asterisk.org/pub/security/AST-2009-006-1.6.1.diff.txt	1.6.1

Links	http://www.rfc-editor.org/authors/rfc5456.txt https://issues.asterisk.org/view.php?id=12912 http://www.beyondsecurity.com/ssd.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-2009-006.pdf and http://downloads.digium.com/pub/security/AST-2009-006.html

Revision History		
Date	**Editor**	**Revisions Made**
2009-09-03	Russell Bryant	Initial release