Product	Asterisk
Summary	Asterisk IAX 'POKE' resource exhaustion
Nature of Advisory	Denial of service
Susceptibility	Remote Unauthenticated Sessions
Severity	Critical
Exploits Known	Yes
Reported On	July 18, 2008
Reported By	Jeremy McNamara < jj AT nufone DOT net >
Posted On	July 22, 2008
Last Updated On	December 12, 2008
Advisory Contact	Tilghman Lesher < tlesher AT digium DOT com >
CVE Name	CVE-2008-3263

Description	By flooding an Asterisk server with IAX2 'POKE' requests, an attacker may eat up all call numbers associated with the IAX2 protocol on an Asterisk server and prevent other IAX2 calls from getting through. Due to the nature of the protocol, IAX2 POKE calls will expect an ACK packet in response to the PONG packet sent in response to the POKE. While waiting for this ACK packet, this dialog consumes an IAX2 call number, as the ACK packet must contain the same call number as was allocated and sent in the PONG.

Resolution	The implementation has been changed to no longer allocate an IAX2 call number for POKE requests. Instead, call number 1 has been reserved for all responses to POKE requests, and ACK packets referencing call number 1 will be silently dropped.

Commentary	This vulnerability was reported to us without exploit code, less than two days before public release, with exploit code. Additionally, we were not informed of the public release of the exploit code and only learned this fact from a third party. We reiterate that this is irresponsible security disclosure, and we recommend that in the future, adequate time be given to fix any such vulnerability. Recommended reading: http://www.oisafety.org/guidelines/Guidelines%20for%20Security%20Vulnerability%20Reporting%20and%20Response%20V2.0.pdf **Update:** Since we've heard from a few people who seem to be faulting Jeremy McNamara for irresponsible disclosure, let me just say that Jeremy is the innocent third party in the above paragraph. He sought to tell us prior to the public disclosure even though the researcher responsible apparently did not. That researcher contacted us well after this advisory was published, which was the first

	we'd heard from him. I won't disclose his name here. I think he's learned a valuable lesson both about responsible disclosure, as well as putting one of his friends in the middle of this firestorm. His name isn't that difficult to find, but to avoid the inevitable flames that might erupt, I'll leave it off here. Suffice it to say, Jeremy does not deserve the derision of either the Asterisk or the security communities. If you misunderstood the original advisory and blamed Jeremy, I hope you will take some time to make amends.

Affected Versions		
Product	**Release Series**	
Asterisk Open Source	1.0.x	All versions
Asterisk Open Source	1.2.x	All versions prior to 1.2.30
Asterisk Open Source	1.4.x	All versions prior to 1.4.21.2
Asterisk Addons	1.2.x	Not affected
Asterisk Addons	1.4.x	Not affected
Asterisk Business Edition	A.x.x	All versions
Asterisk Business Edition	B.x.x.x	All versions prior to B.2.5.4
Asterisk Business Edition	C.x.x.x	All versions prior to C.1.10.3
AsteriskNOW	pre-release	All versions
Asterisk Appliance Developer Kit	0.x.x	All versions
s800i (Asterisk Appliance)	1.0.x	All versions prior to 1.2.0.1

Corrected In	
Product	**Release**
Asterisk Open Source	1.2.30.1
Asterisk Open Source	1.4.21.2
Asterisk Business Edition	B.2.5.4
Asterisk Business Edition	C.1.10.3
Asterisk Business Edition	C.2.0.3
s800i (Asterisk Appliance)	1.2.0.1

Patches

URL	Version
http://downloads.digium.com/pub/security/AST-2008-010-1.2.patch	1.2
http://downloads.digium.com/pub/security/AST-2008-010-1.4.patch	1.4

Links	http://www.oisafety.org/guidelines/Guidelines%20for%20Security%20Vulnerability%20Reporting%20and%20Response%20V2.0.pdf
	http://www.securityfocus.com/bid/30321/info

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-2008-010.pdf and http://downloads.digium.com/pub/security/AST-2008-010.html

Revision History		
Date	**Editor**	**Revisions Made**
July 22, 2008	Tilghman Lesher	Initial release
July 22, 2008	Tilghman Lesher	Revised C.1 version numbers
July 24, 2008	Tilghman Lesher	Released 1.2.30.1 to account for an error in patching
July 28, 2008	Tilghman Lesher	Updated commentary to make it clear that Jeremy was not at fault.
December 12, 2008	Tilghman Lesher	Added patches