Asterisk Project Security Advisory - AST-2008-005

Product	Asterisk
Summary	HTTP Manager ID is predictable
Nature of Advisory	An attacker could hijack a manager session
Susceptibility	All users using the HTTP manager port
Severity	Minor
Exploits Known	No
Reported On	February 25, 2008
Reported By	Dino A. Dai Zovi < ddz AT theta44 DOT org >
Posted On	March 18, 2008
Last Updated On	December 12, 2008
Advisory Contact	Tilghman Lesher < tlesher AT digium DOT com >
CVE Name	CVE-2008-1390

Description	Due to the way that manager IDs are calculated, this 32-bit integer is likely to have a much larger than average number of 1s, which greatly reduces the number of guesses an attacker would have to make to successfully predict the manager ID, which is used across multiple HTTP queries to hold manager state. "The issue is the generation of session ids in the AsteriskGUI HTTP server. When using Glibc, the implementation and state of rand() and random() is shared. Asterisk uses random() to issue MD5 digest authentication challenges and rand() bitwise-ORed with a malloc'd pointer to generate AsteriskGUI session identifiers. An attacker can synchronize with random() by retrieving 32 successive challenges and predict all subsequent output of calls to random() and rand(). Because a pointer returned by malloc has at best 21 bits of entropy, the attacker will on average only need to guess 1448 session identifiers in order to steal an established session. "The crux of the problem is that under Glibc, the implementation of rand() and random() is shared. rand() is just an alias to random(). This means that they all come from the same randomizer with the same state. "A remote attacker can synchronize with all subsequent output of a remote system's random() state by just observing or retrieving 32 successive outputs. They can easily do this by generating 32 MD5 digest authentication challenges. At this point, they will be able to predict all subsequent output of random() and rand(). "The memory address returned by calloc() is also not sufficiently random. In practice, it will be in low memory, immediately following the executable.

	In addition, the buffer returned will be 8-byte aligned. This means that the high order 8 bits and low order 3 bits will always be zero. Finally, this value is bitwise ORed with the output of random(), so any bits that are set will be preserved. "An attacker will only have to guess 2^N session ids, where N is the number of zeros in the number return by random() between bit positions 3 and 24. On average, this will be 1448 guesses. "However, an attacker can do better than this by consuming challenges until the following number output by random() has many 1's in those significant bit positions."

Resolution	To mitigate this attack, the two values are now XORed together. This will increase the entropy to approximately 2^21, which is far more difficult to predict, especially given that the random number generator is used for other purposes in Asterisk, not just manager HTTP session ID generation. Upgrade to SVN revision 104704 or greater, or upgrade to one of the releases below. That the random number generator is used for other things makes this attack extremely difficult and unlikely, so we will not produce a separate release for this security advisory.

Affected Versions		
Product	**Release Series**	
Asterisk Open Source	1.0.x	Not affected
Asterisk Open Source	1.2.x	Not affected
Asterisk Open Source	1.4.x	All versions prior to 1.4.19-rc3
Asterisk Open Source	1.6.x	All versions prior to 1.6.0-beta6
Asterisk Business Edition	A.x.x	Not affected
Asterisk Business Edition	B.x.x	Not affected
Asterisk Business Edition	C.x.x	All versions prior to C.1.6
AsteriskNOW	pre-release	All versions prior to 1.0.2
Asterisk Appliance Developer Kit	SVN	All revisions prior to 104704
s800i (Asterisk Appliance)	1.0.x	All versions prior to 1.1.0.2

Corrected In	
Product	**Release**
Asterisk Open Source	1.4.19-rc3, 1.6.0-beta6
Asterisk Business Edition	C.1.6
AsteriskNOW	1.0.2
Asterisk Appliance Developer Kit	Asterisk 1.4 revision 104704
s800i (Asterisk Appliance)	1.1.0.2

Patches	
URL	**Version**
http://downloads.digium.com/pub/security/AST-2008-005-1.2.patch	1.2
http://downloads.digium.com/pub/security/AST-2008-005-1.4.patch	1.4

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-2008-005.pdf and http://downloads.digium.com/pub/security/AST-2008-005.html

Revision History		
Date	**Editor**	**Revisions Made**
2008-03-18	Tilghman Lesher	Initial release
2008-12-12	Tilghman Lesher	Add patches