Product	Asterisk
Summary	File Descriptor Resource Exhaustion
Nature of Advisory	Denial of Service
Susceptibility	Remote Unauthenticated TCP Based Sessions (TCP SIP, Skinny, Asterisk Manager Interface, and HTTP sessions)
Severity	Moderate
Exploits Known	Yes
Reported On	March 18, 2011
Reported By	Tzafrir Cohen < tzafrir.cohen AT xorcom DOT com >
Posted On	April 21, 2011
Last Updated On	April 21, 2011
Advisory Contact	Matthew Nicholson <mnicholson@digium.com>
CVE Name	CVE-2011-1507

Description	On systems that have the Asterisk Manager Interface, Skinny, SIP over TCP, or the built in HTTP server enabled, it is possible for an attacker to open as many connections to asterisk as he wishes. This will cause Asterisk to run out of available file descriptors and stop processing any new calls. Additionally, disk space can be exhausted as Asterisk logs failures to open new file descriptors.

Resolution	Asterisk can now limit the number of unauthenticated connections to each vulnerable interface and can also limit the time unauthenticated clients will remain connected for some interfaces. This will prevent vulnerable interfaces from using up all available file descriptors. Care should be taken when setting the connection limits so that the combined total of allowed unauthenticated sessions from each service is not more than the file descriptor limit for the Asterisk process. The file descriptor limit can be checked (and set) using the “ulimit -n” command for the process' limit and the “/proc/sys/fs/file-max” file (on Linux) for the system's limit. It will still be possible for an attacker to deny service to each of the vulnerable services individually. To mitigate this risk, vulnerable services should be run behind a firewall that can detect and prevent DoS attacks. In addition to using a firewall to filter traffic, vulnerable systems can be protected by disabling the vulnerable services in their respective configuration files.

Affected Versions		
Product	**Release Series**	
Asterisk Open Source	1.4.x	All versions
Asterisk Open Source	1.6.1.x	All versions
Asterisk Open Source	1.6.2.x	All versions
Asterisk Open Source	1.8.x	All versions
Asterisk Business Edition	C.x.x	All versions

Corrected In	
Product	**Release**
Asterisk Open Source	1.4.40.1, 1.6.1.25, 1.6.2.17.3, 1.8.3.3
Asterisk Business Edition	C.3.6.4

Patches	
URL	**Branch**
http://downloads.asterisk.org/pub/security/AST-2011-005-1.4.diff	1.4
http://downloads.asterisk.org/pub/security/AST-2011-005-1.6.1.diff	1.6.1
http://downloads.asterisk.org/pub/security/AST-2011-005-1.6.2.diff	1.6.2
http://downloads.asterisk.org/pub/security/AST-2011-005-1.8.diff	1.8

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-2011-005.pdf and http://downloads.digium.com/pub/security/AST-2011-005.html

Revision History		
Date	**Editor**	**Revisions Made**
04/21/11	Matthew Nicholson	Initial version