| | |
|---|---|
| **Product** | Asterisk |
| **Summary** | Remote crash vulnerability in Skinny channel driver |
| **Nature of Advisory** | Denial of Service |
| **Susceptibility** | Remote Unauthenticated Sessions |
| **Severity** | Critical |
| **Exploits Known** | No |
| **Reported On** | July 13, 2007 |
| **Reported By** | Will Drewry, Google Security Team |
| **Posted On** | July 17, 2007 |
| **Last Updated On** | August 21, 2007 |
| **Advisory Contact** | Jason Parker <jparker@digium.com> |
| **CVE Name** | CVE-2007-3764 |

| | |
|---|---|
| **Description** | The Asterisk Skinny channel driver, chan_skinny, has a remotely exploitable crash vulnerability. A segfault can occur when Asterisk receives a packet where the claimed length of the data is between 0 and 3, followed by *length* + 4 or more bytes, due to an overly large memcpy. The side effects of this extremely large memcpy have not been investigated. |

| | |
|---|---|
| **Resolution** | All users that have chan_skinny enabled should upgrade to the appropriate version listed in the corrected in section of this advisory. As a workaround, users who do not require chan_skinny may add the line “noload => chan_skinny.so” (without quotes) to /etc/asterisk/modules.conf, and restart Asterisk. |

| Affected Versions | | |
|---|---|---|
| **Product** | **Release Series** | |
| Asterisk Open Source | 1.0.x | All versions |
| Asterisk Open Source | 1.2.x | All versions prior to 1.2.22 |
| Asterisk Open Source | 1.4.x | All versions prior to 1.4.8 |
| Asterisk Business Edition | A.x.x | All versions |
| Asterisk Business Edition | B.x.x | All versions prior to B.2.2.1 |
| AsteriskNOW | pre-release | All versions prior to beta7 |
| Asterisk Appliance Developer Kit | 0.x.x | All versions prior to 0.5.0 |
| s800i (Asterisk Appliance) | 1.0.x | All versions prior to 1.0.2 |

| Corrected In | |
|---|---|
| **Product** | **Release** |
| Asterisk Open Source | 1.2.22 and 1.4.8, available from http://downloads.digium.com/pub/telephony/asterisk |
| Asterisk Business Edition | B.2.2.1, available from the Asterisk Business Edition user portal on http://www.digium.com or via Digium Technical Support |
| AsteriskNOW | Beta7, available from http://www.asterisknow.org/. Beta5 and Beta6 users can update using the system update feature in the appliance control panel. |
| Asterisk Appliance Developer Kit | 0.5.0, available from http://downloads.digium.com/pub/telephony/aadk/ |
| s800i (Asterisk Appliance) | 1.0.2 |

| 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-2007-016.pdf and http://downloads.digium.com/pub/asa/AST-2007-016.html.

| Revision History |
|---|

| Date | Editor | Revisions Made |
|---|---|---|
| July 17, 2007 | jparker@digium.com | Initial Release |
| August 21, 2007 | russell@digium.com | Changed name prefix from ASA to AST, changed ftp.digium.com to downloads.digium.com |