| | |
|---|---|
| **Product** | Asterisk |
| **Summary** | Traffic amplification in IAX2 firmware provisioning system |
| **Nature of Advisory** | Traffic amplification attack |
| **Susceptibility** | Remote unauthenticated sessions |
| **Severity** | Critical |
| **Exploits Known** | No |
| **Reported On** | July 18, 2008 |
| **Reported By** | Tilghman Lesher < tlesher AT digium DOT com > |
| **Posted On** | July 22, 2008 |
| **Last Updated On** | December 12, 2008 |
| **Advisory Contact** | Tilghman Lesher < tlesher AT digium DOT com > |
| **CVE Name** | CVE-2008-3264 |

| | |
|---|---|
| **Description** | An attacker may request an Asterisk server to send part of a firmware image. However, as this firmware download protocol does not initiate a handshake, the source address may be spoofed. Therefore, an IAX2 FWDOWNL request for a firmware file may consume as little as 40 bytes, yet produces a 1040 byte response. Coupled with multiple geographically diverse Asterisk servers, an attacker may flood an victim site with unwanted firmware packets. |

| | |
|---|---|
| **Workaround** | The only device which used this firmware upgrade procedure was the IAXy ATA device, and the last firmware upgrade was more than 18 months ago. It is unlikely that any IAXy devices in use today still need the last firmware upgrade. Therefore, deleting the firmware image from the directory where it is served from and sending a reload event to the Asterisk server is sufficient to purge the firmware image from the Asterisk server's memory. An Asterisk server which is unable to serve out the requested firmware image will reply to any such request with a much smaller REJECT packet, which is smaller than even the FWDOWNL packet. |

| | |
|---|---|
| **Resolution** | This firmware download procedure has been disabled by default in Asterisk. If you should still need to upgrade IAXys in the field, there is an option 'allowfwdownload' which can be enabled. However, due to the reasons specified on the Workaround section, it is recommended that you leave this option disabled and enable it only on secure internal networks when an IAXy is initially provisioned. |

| 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 | All versions prior to B.2.5.4 |
| Asterisk Business Edition | C.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 |
| 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-2008-011-1.2.patch | 1.2 |
| http://downloads.digium.com/pub/security/AST-2008-011-1.4.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-2008-011.pdf and http://downloads.digium.com/pub/security/AST-2008-011.html

| Revision History | | |
|---|---|---|
| **Date** | **Editor** | **Revisions Made** |
| July 22, 2008 | Tilghman Lesher | Initial release |
| July 22, 2008 | Tilghman Lesher | Revised C.1 version numbers |
| December 12, 2008 | Tilghman Lesher | Added patches |