

[NEWS] IAX2 Users can Cause Unauthorized Data Disclosure

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2007-05/msg00011.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxxxx>
 - *Date:* 7 May 2007 13:01:36 +0200
-

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>
-- promotion

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.
<http://www.securiteam.com/maillinglist.html>

IAX2 Users can Cause Unauthorized Data Disclosure

SUMMARY

The IAX2 implementation of Asterisk has been found to contain a vulnerability that would allow a remote attacker to disclose the content of the stack memory and potentially cause the product to crash by sending it a malformed text frame.

DETAILS

Vulnerable Systems:

- * Asterisk Open Source versions prior to 1.2.19
- * Asterisk Open Source versions prior to 1.4.4
- * Asterisk Business Edition versions A.x.x
- * Asterisk Business Edition versions prior to B.2.1
- * AsteriskNOW versions prior to and include Beta 5
- * Asterisk Appliance Developer Kit versions prior 0.4.1

Immune Systems:

- * Asterisk Open Source version 1.2.19
- * Asterisk Open Source version 1.4.4
- * Asterisk Business Edition version B.2.1

[NEWS] IAX2 Users can Cause Unauthorized Data Disclosure

- * AsteriskNOW version Beta 6
- * Asterisk Appliance Developer Kit version 0.4.1

chan_iax2 assumes that the content of a text frame is a NULL terminated string (C style), and when time comes to forward the string it uses strlen to determine the message length. If you send a frame without a 0 byte in it, Asterisk forwards a frame that includes the sent data and some extra (presumably heap) data. If an attacker were lucky, the extra data could contain something interesting. Or conceivably it could cause a segmentation violation.

Resolution:

Asterisk code has been modified to enforce null-termination of incoming text frames received by the IAX2 channel driver (chan_iax2). When text frames are received without null-termination, this may result in the last byte of data in the frame being lost, if the IAX2 reception process does not have space in its receive buffer to add a null character.

As this vulnerability is of 'low' severity, it does not justify new releases of Asterisk solely for mitigating its impact. The fix for this vulnerability has been committed to the Asterisk Subversion source code repositories and is available to all users who wish to upgrade to a prerelease checkout of the respective development branch for their release series of Asterisk. All other users can upgrade when the next regularly scheduled release of their product is produced.

CVE Information:

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-2488>>
 CVE-2007-2488

ADDITIONAL INFORMATION

The information has been provided by <<mailto:tim@xxxxxxxxxx>> Tim Panton, Mexuar and <<mailto:birgit@xxxxxxxxxxxxxxxx>> Birgit Arkesteijn, Westhawk .

The original article can be found at:

<<http://ftp.digium.com/pub/asa/ASA-2007-013.pdf>>
<http://ftp.digium.com/pub/asa/ASA-2007-013.pdf>

=====

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:

list-unsubscribe@xxxxxxxxxxxxxxxx

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@xxxxxxxxxxxxxxxx

=====

[NEWS] IAX2 Users can Cause Unauthorized Data Disclosure

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.