

[UNIX] Asterisk SIP Denial Of Service Vulnerability (INVITE)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2007-03/msg00042.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxxx>
 - *Date:* 22 Mar 2007 16:26:14 +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>

Asterisk SIP Denial Of Service Vulnerability (INVITE)

SUMMARY

AsteriskR is "a complete IP PBX in software. It runs on a wide variety of operating systems including Linux, Mac OS X, OpenBSD, FreeBSD and Sun Solaris and provides all of the features you would expect from a PBX including many advanced features that are often associated with high end (and high cost) proprietary PBXs".

After sending a crafted INVITE message the software finish abruptly its execution with a Segmentation Fault provoking a Denial of Service (DoS) in all the services provided by the entity.

DETAILS

Vulnerable Systems:

- * Asterisk versions 1.2.14, 1.2.15, 1.2.16
- * Asterisk version 1.4.1
- * Previous versions are also suspected.

Immune Systems:

- * Asterisk version 1.2.17

[UNIX] Asterisk SIP Denial Of Service Vulnerability (INVITE)

- * Asterisk version 1.4.2
- * Repository trunk version to date (13/03/2007)

After sending a crafted message the software crash abruptly. The message in this case is an anonymous INVITE where the SDP contains 2 connection headers. The first one must be valid and the second not where the IP address should be invalid. The callee needs not to be a valid user or dialplan. In case where asterisk is set to disallow anonymous call, a valid user and password should be known, and while responding the corresponding INVITE challenge the information should be crafted as above. After this crafted SIP INVITE message, the affected software crash immediately.

A remote individual can remotely crash and perform a Denial of Service(DoS) attack in all the services provided by the software by sending one crafted SIP INVITE message. This is conceptually similar to the "ping of death".

ADDITIONAL INFORMATION

The information has been provided by <<mailto:state@xxxxxxxx>> Radu State.

=====

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

=====
=====

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.