

[UNIX] Asterisk SIP DoS Vulnerability (Empty REGISTER)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2007-03/msg00031.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxx>
 - *Date:* 13 Mar 2007 15:49:18 +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 DoS Vulnerability (Empty REGISTER)

SUMMARY

" <<http://www.asterisk.org/>> Asterisk is the most popular and extensible open source telephone system in the world, offering flexibility, functionality and features not available in advanced, high-end (high-cost) proprietary business systems. Asterisk is a complete IP PBX (private branch exchange) for businesses, and can be downloaded for free." Due to bad handling by Asterisk's SIP parser, a remote attacker can cause the product to crash by sending it a malformed SIP REGISTER request.

DETAILS

Vulnerable Systems:

* Asterisk versions 1.2.15 and 1.4.0, and earlier.

Asterisk crashes when handed an otherwise valid request message but with no URI and no SIP-version in the request-line of the message. For example, "REGISTER\r\n <other valid SIP headers>". The crash is due to a null pointer dereference, and does not appear to be otherwise exploitable.

Vendor Status:

[UNIX] Asterisk SIP DoS Vulnerability (Empty REGISTER)

Fixed in releases 1.2.16 and 1.4.1.

Available from <<http://www.asterisk.org>> <http://www.asterisk.org>

Disclosure Timeline:

- * March 1, 2007 – First contact with vendor
- * March 2, 2007 – Vendor acknowledges vulnerability
- * March 7, 2007 – Advisory released
- * March 9, 2007 – Advisory updated with correct dates

ADDITIONAL INFORMATION

The information has been provided by musecurity.

The original article can be found at:

<<http://labs.musecurity.com/advisories/MU-200703-01.txt>>

<http://labs.musecurity.com/advisories/MU-200703-01.txt>

=====

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@xxxxxxxxxxxxxxx

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

=====

=====

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.