

[UNIX] Remote DoS in libevent DNS Parsing

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2007-02/msg00064.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxx>
 - *Date:* 20 Feb 2007 14:57:12 +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>

Remote DoS in libevent DNS Parsing

SUMMARY

The <<http://monkey.org/~provos/libevent/>> libevent "API provides a mechanism to execute a callback function when a specific event occurs on a file descriptor or after a timeout has been reached. Furthermore, libevent also support callbacks due to signals or regular timeouts".

libevent is meant to replace the event loop found in event driven network servers. An application just needs to call `event_dispatch()` and then add or remove events dynamically without having to change the event loop. Currently, libevent supports `/dev/poll`, `kqueue(2)`, `select(2)`, `poll(2)` and `epoll(4)`.

Recently, support for non-blocking DNS resolution was added to libevent.

A vulnerability in the way libevent handles DNS requests allows attackers to cause the program to no longer respond to legitimate requests.

DETAILS

Vulnerable Systems:

* libevent version 1.2 up to version 1.2a

[UNIX] Remote DoS in libevent DNS Parsing

Immune Systems:

* libevent version 1.3

A bug exists in the parsing of DNS responses in libevent, specifically in the handling of label pointers. Label pointers in DNS are meant to cut down on redundant information and overall response size by allowing a label to reference an arbitrary byte offset in the packet. If a pointer references its own offset, a pointer loop is formed. libevent's parsing code does not properly handle such pointer loops.

Impact

A malicious resolver, authoritative server, or inline attacker can send a DNS reply containing a pointer loop, causing libevent's DNS parsing to enter an endless loop, effectively DoS'ing the service.

Resolution

Applications utilizing the DNS resolution functionality of libevent should upgrade to version ≥ 1.3 .

ADDITIONAL INFORMATION

The information has been provided by <mailto:jon@xxxxxxxxxxxxxx> Jon Oberheide.

=====

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@xxxxxxxxxxxxxx

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

=====

=====

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.