

[UNIX] Denial of Service in Leafnode

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-09/0023.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 09/08/03

To: list@securiteam.com

Date: 8 Sep 2003 14:05:43 +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>

Denial of Service in Leafnode

SUMMARY

<<http://www.leafnode.org/>> Leafnode is a store-and-forward proxy for Usenet news, it uses the network news transfer protocol (NNTP). It consists of several collaborating programs, the server part is usually started by inetd, xinetd, or tcpserver, the client part is usually started by cron or manually.

A vulnerability was found in the fetchnews program (the NNTP client) that may under some circumstances cause wait for input that never arrives, fetchnews "hangs". This hang does not cost CPU.

This bug was not deemed security relevant at first, but as it can be triggered from the outside, by providing malformed (non-RFC-1036) Usenet news articles, and because it then stops unattended systems from functioning, it was decided to release this security announcement.

DETAILS

Vulnerable systems:

* Leafnode 1.9.3 (1999) up to 1.9.41 (2003)

Immune systems:

Securiteam: [UNIX] Denial of Service in Leafnode

* Leafnode 1.9.42 and newer

Impact:

As only one fetchnews program can run at a time, subsequently started fetchnews and texpire programs will terminate immediately. This means that the news base will no longer be updated. Older articles will no longer expire, until the hanging fetchnews process gets unstuck, usually through a manual "kill" command or a reboot.

Workaround:

No reliable workaround possible.

NOTE: Killing fetchnews before completion leaves stale data on disk and is therefore not deemed reliable, although it relieves the immediate "cannot start texpire or fetchnews" condition.

Solution:

Upgrade your Leafnode package to version 1.9.42 or later. At this time, Leafnode 1.9.43 is the up-to-date stable release.

Note that Leafnode 1.9.X versions are deemed stable, and it is usually best to go for the latest released 1.9.X version to have all the other bug fixes as well. No broken-out version of this patch will be provided, distributors are urged to update to the latest Leafnode version.

Leafnode 1.9.43 is available from sourceforge:

http://sourceforge.net/project/showfiles.php?group_id=57767&release_id=182196
http://sourceforge.net/project/showfiles.php?group_id=57767&release_id=182196

This policy of not providing a broken-out patch may generate a conflict with some distribution's post-release update policies.

As the current Leafnode maintainer, Matthias Andree does not have financial and time resources to provide support for any but the latest released version.

People keep reporting bugs about leafnode-1.9.33, 1.9.24, or 1.9.19, which is a waste of time for the user and the Leafnode maintainer.

ADDITIONAL INFORMATION

The information has been provided by Joshua Crawford.

=====

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@securiteam.com

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

Securiteam: [UNIX] Denial of Service in Leafnode

=====
=====

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.