

[TOOL] KArp – Linux Kernel ARP Hijacking Patch

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2006-03/msg00054.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxxxx>
 - *Date:* 20 Mar 2006 12:23:13 +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>

KArp – Linux Kernel ARP Hijacking Patch

SUMMARY

DETAILS

KArp is a linux patch that allows one to implement ARP hijacking in the kernel, but control it easily via userland. You may configure, enable and disable KArp via ProcFS or the sysctl mechanism.

KArp is implemented almost on the device driver level. Any ethernet driver (including 802.11 drivers) is supported. The KArp code is lower than the actual ARP code in the network stack, and thus will respond to ARP requests faster than a normal machine running a normal network stack, even if the machine we're spoofing has a CPU twice as fast as ours!

Currently, linux-2.6.16-rc6 is supported, but KArp is easy to port to other releases.

This code was written to help facilitate a MiM project.

WARNING

[TOOL] KArp – Linux Kernel ARP Hijacking Patch

KArp was written to beat the race in responding to an ARP Request from a target (victim) machine. It is not meant as a tool to flood a victim with ARP information.

This means that some operating systems (MacOSX) that ingest unsolicited ARP responses may still obtain the actual MAC address of the machine we're impersonating. Linux, however, only accepts the fastest response. If you want to flood a machine with fake ARP responses, use a userland tool. However, there may be a delay mechanism implemented later that allows us to lose the race for lazy operating systems, forcing them to ingest our address.

To download the patch:

<<http://aversion.net/~north/karp/patch-2.6.16-rc6-karp>>
<http://aversion.net/~north/karp/patch-2.6.16-rc6-karp>

ADDITIONAL INFORMATION

The information has been provided by <<mailto:don.bailey@xxxxxxxxxx>> Don Bailey.

To keep updated with the tool visit the project's homepage at:

<<http://aversion.net/~north/karp/>> <http://aversion.net/~north/karp/>

=====

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.