

# [UNIX] OpenBSD Kernel Panic While Processing IPsec Link2 Option

**Source:** <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-09/0009.html>

---

**From:** SecuriTeam ([support\\_at\\_securiteam.com](mailto:support_at_securiteam.com))

**Date:** 09/02/04

To: [list@securiteam.com](mailto:list@securiteam.com)

Date: 2 Sep 2004 14:05:57 +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>

-----

OpenBSD Kernel Panic While Processing IPsec Link2 Option

---

## SUMMARY

A bug in the way the OpenBSD kernel handles ICMP packets while the link2 option is set for IPsec processing leaves the system vulnerable to a single ICMP packet attack able to crash the kernel.

## DETAILS

Vulnerable Systems:

- \* OpenBSD version 3.5

An OpenBSD system configured as a gateway between two networks might be vulnerable to a specific attack that can crash the kernel if bridging is enabled and the link2 option is given for IPsec processing. In an event that a malformed ICMP echo request packet arrives from a host on network A with a destination of a host on network B, the OpenBSD kernel will crash and cause a kernel panic.

No core file is generated. If the DDB\_PANIC option is set, the machine reboots upon receipt of the ICMP echo request. The commands that lead to the vulnerable situations are as follows:

## Securiteam: [UNIX] OpenBSD Kernel Panic While Processing IPsec Link2 Option

```
# ifconfig bridge0 create
# brconfig bridge0 add fxp0 add fxp1 up
# brconfig bridge0 link2
```

Naturally, in order to configure the system in such a manner, a user would have to have root access on the system.

The problem was observed on a test network and was reproduced as well on a VMWare network.

### Patch Availability:

The OpenBSD team was contacted and a patch was introduced to the CVS within 12 hours, an errata is available at:

<<http://www.openbsd.org/errata34.html>>

<http://www.openbsd.org/errata34.html>. The patch code is listed below and is also available from

<[ftp://ftp.openbsd.org/pub/OpenBSD/patches/3.4/common/028\\_bridge.patch](ftp://ftp.openbsd.org/pub/OpenBSD/patches/3.4/common/028_bridge.patch)>

[ftp://ftp.openbsd.org/pub/OpenBSD/patches/3.4/common/028\\_bridge.patch](ftp://ftp.openbsd.org/pub/OpenBSD/patches/3.4/common/028_bridge.patch):

Index: sys/net/if\_bridge.c

```
=====
RCS file: /cvs/src/sys/net/if_bridge.c,v
retrieving revision 1.136
diff -u -r1.136 if_bridge.c
--- sys/net/if_bridge.c 21 Jun 2004 23:50:36 -0000 1.136
+++ sys/net/if_bridge.c 18 Aug 2004 09:29:04 -0000
@@ -2275,9 +2275,9 @@
         splx(s);
         return (1);
     } else {
+ splx(s);
     skiplookup:
         /* XXX do an input policy lookup */
- splx(s);
         return (0);
     }
 } else { /* Outgoing from the bridge. */
```

### ADDITIONAL INFORMATION

The information has been provided by <<mailto:vafa@hush.ai>> Vafa Izadinia.

=====

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](mailto:list-unsubscribe@securiteam.com)

In order to subscribe to the mailing list, simply forward this email to: [list-subscribe@securiteam.com](mailto:list-subscribe@securiteam.com)

=====

## Securiteam: [UNIX] OpenBSD Kernel Panic While Processing IPsec Link2 Option

### 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.