

# [UNIX] Local Netfilter / IPTables IP Queue PID Wrap Flaw

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-12/0028.html>

---

*From:* [support@securiteam.com](mailto:support@securiteam.com)

*Date:* 12/08/02

From: [support@securiteam.com](mailto:support@securiteam.com)

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

Date: 8 Dec 2002 23:23:33 +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

Beyond Security would like to welcome Tiscali World Online to our service provider team.

For more info on their service offering IP-Secure, please visit [http://www.worldonline.co.za/services/work\\_ip.asp](http://www.worldonline.co.za/services/work_ip.asp)

-----

Local Netfilter / IPTables IP Queue PID Wrap Flaw

---

## SUMMARY

A security vulnerability in Netfilter/IPTables will allow under certain circumstances, an unprivileged local user to be able to read a limited amount of arbitrary IPv4 or IPv6 traffic.

## DETAILS

Vulnerable systems:

Linux 2.4 kernels up to and including 2.4.19, and Linux 2.5 kernels up to and including 2.5.31, where Netfilter / IPTables is enabled, and where either of the experimental IP queuing modules (ip\_queue, ip6\_queue) are in use.

Immune systems:

- \* Linux kernels version 2.4.20 (stable) and up
- \* Linux kernels version 2.5.32 (development) and up

Under Linux 2.4 and 2.5, an experimental IP packet queuing feature is available as part of Netfilter / IPTables. This consists of kernel modules and a userspace library which allow userspace mediation and modification of IPv4 and IPv6 packets.

## Securiteam: [UNIX] Local Netfilter / IPTables IP Queue PID Wrap Flaw

A userspace mediation process must normally be privileged (requiring NET\_ADMIN capability) to process packets from the kernel. To commence mediating packets, a userspace process typically sends a Netlink message to the associated kernel module, specifying queuing parameters. The kernel module captures the UNIX process ID (PID) of the process to ensure reliable queuing and delivery of packets.

If the privileged mediation process exits, an unprivileged process re-using the same PID may be able to receive a limited amount of network traffic.

This would only occur if no network traffic was queued between the exit of the privileged process and the establishment of the unprivileged process, as the kernel module will reset the queuing session upon transmission error to userspace.

The kernel module will only transmit a limited number of packets to the userspace process without acknowledgment. As all transmissions from userspace to the kernel module require NET\_ADMIN capability, the unprivileged process will not be able to acknowledge packets. Thus, the maximum number of packets that the unprivileged process can read is limited to the queue length (default 1024 packets). The unprivileged process can also only read packets which have been selected for queuing via IPTables by a privileged process.

This flaw is theorized to be difficult and somewhat invasive to exploit, probably requiring a combined use of DoS attacks. It was discovered by the author of the code, and no exploits are known to exist.

Fixing the flaw involved implementing a reliable mechanism for detecting when the Netlink control socket of a privileged mediation process is closed, and resetting the kernel queuing session state upon such events.

### ADDITIONAL INFORMATION

The information has been provided by <<mailto:jmorris@intercode.com.au>>  
James Morris.

=====

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)

=====  
=====

### 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.