

Securiteam: [NEWS] Flawed Outbound Packet Filtering in Various Personal Firewalls

# [NEWS] Flawed Outbound Packet Filtering in Various Personal Firewalls

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2001-12/0042.html>

---

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

*Date:* 12/12/01

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

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

Date: Wed, 12 Dec 2001 20:16:17 +0100 (CET)

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

When was the last time you checked your server's security?

How about a monthly report?

<http://www.AutomatedScanning.com> -- Know that you're safe.

-----

Flawed Outbound Packet Filtering in Various Personal Firewalls

---

## SUMMARY

Outbound filtering in personal firewalls does not block packets that are generated by protocol stacks other than the default Microsoft stack. This enables Trojans that generate packets using non standard protocol adaptors to send outbound information bypassing the firewall rules.

## DETAILS

Known vulnerable firewalls:

ZoneAlarm and ZoneAlarm Pro as of their current revisions

Tiny Personal Firewall

A security flaw has been found in at least two personal firewalls causing them to not "see" the TCP packets that are generated using a "non-standard" protocol adapter.

Furthermore, the "Lock" or "Block All" settings of those firewalls are also ineffective against TCP packets from non-standard protocol adapters.

Vendor responses:

ZoneLabs:

## Securiteam: [NEWS] Flawed Outbound Packet Filtering in Various Personal Firewalls

ZoneLabs was initially contacted regarding this issue on November 9th. Since that time, A few sporadic updates have been received on their progress in fixing this issue. As of the present time, the supplied "fix" will silently drop all TCP packets not originating from the standard Windows TCP protocol adapter. This shouldn't be considered an expected behavior, but rather a quick patch.

Tiny software:

Tiny was also contacted in mid–November, but no reply was received. They were recently re–contacted, and they have now acknowledged that the problem exists, and have stated that they intend to block "non–standard" protocol access to NDIS, but have yet to reply about how this will be accomplished.

Note:

Other personal firewalls might very well be susceptible to this same problem.

Also troubling is the fact that, in both cases, specially crafted packets can be sent to a machine which an application can sniff off the wire. These packets are ignored by the personal firewalls and there is no warning to the end user. This makes two–way communication possible with a machine, even when its firewall is set to "Lock" or "Block All" network traffic.

Exploit:

An application, demonstrating this vulnerability is available at:

<http://www.hackbusters.net/ob.html> > <http://www.hackbusters.net/ob.html>

### ADDITIONAL INFORMATION

The information has been provided by <mailto:[tliston@premmag.com](mailto:tliston@premmag.com)> Tom Liston and <mailto:[tsmith@zonelabs.com](mailto:tsmith@zonelabs.com)> Te Smith.

=====

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.

---

• *Previous message:* [support@securiteam.com](mailto:support@securiteam.com): "[TOOL] SQLAT – SQL Auditing Tools"

Securiteam: [NEWS] Flawed Outbound Packet Filtering in Various Personal Firewalls

- *Messages sorted by:* [ date ] [ thread ] [ subject ] [ author ] [ attachment ]