

# [NEWS] Bypassing Cisco SNMP Access Lists Using Spoofed SNMP Requests

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-08/0034.html>

---

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

*Date:* 08/08/05

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

Date: 8 Aug 2005 17:32:14 +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>

-----

Bypassing Cisco SNMP Access Lists Using Spoofed SNMP Requests

---

## SUMMARY

Under certain conditions, it is possible to bypass the SNMP ACL on Cisco routers and gain ANMP Read / Write privileges.

## DETAILS

In order to gain R/W SNMP access on the router, the following conditions must exist:

- a) RW community string is known
- b) Access list policy is known
- c) Access to the SNMP RW command will occur from the a.b.c.d network (External).
- d) No access lists present on TFTP server address.

Under these conditions, if the server holds an ACL like:

```
access-list 1 permit 192.168.1.0 0.0.0.255
snmp-server community public RO
snmp-server community datest RW 1
```

By spoofing an SNMP packet, it is possible to bypass the ACL. The idea is

## Securiteam: [NEWS] Bypassing Cisco SNMP Access Lists Using Spoofed SNMP Requests

to spoof a packet with a different source IP than the attacker has or more accurately, a source IP which is allowed by the Router SNMP ACL.

Workarounds:

Enforce an ACL on the TFTP used in conjunction with the router, or disable SMNP if possible.

### ADDITIONAL INFORMATION

The information has been provided by <mailto:mati@see-security.com> muts.

The original article can be found at:

<[http://new.remote-exploit.org/index.php/SNMP\\_Spoof](http://new.remote-exploit.org/index.php/SNMP_Spoof)>

[http://new.remote-exploit.org/index.php/SNMP\\_Spoof](http://new.remote-exploit.org/index.php/SNMP_Spoof)

=====

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

=====

=====

### 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.