

# [NEWS] Multiple Looking-Glass Input Vulnerabilities

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2001-10/0062.html>

---

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

*Date:* 10/23/01

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

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

Subject: [NEWS] Multiple Looking-Glass Input Vulnerabilities

Message-Id: <20011022220943.99E39138C9@mail.der-keiler.de>

Date: Tue, 23 Oct 2001 00:09:43 +0200 (CEST)

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.

-----

## Multiple Looking-Glass Input Vulnerabilities

---

### SUMMARY

There is a flaw in many looking-glasses (most of them based on the nitrous-digex one) that allows attackers to gather information about the network that was not intentionally provided. This happens because the looking-glass (which is written in Perl) doesn't check the input properly for the validity of the input address.

### DETAILS

Example:

When clicking bgp, to check an address in the bgp table, the attacker can enter, instead of an ip address, the word "nei"(or neighbors) and all bgp neighbors will be fully visible. In fact, any valid argument in Cisco IOS following 'sh ip bgp' can be entered.

Another example:

<sh ip bgp> paths gives the full path table. This puts some strain on routers and could be used to DoS the router if no proper access security is provided. Various other things can be done

## Securiteam: [NEWS] Multiple Looking-Glass Input Vulnerabilities

Workaround:

Check for a "." in the input.

### ADDITIONAL INFORMATION

The information has been provided by <mailto:[barabas@lokmail.net](mailto:barabas@lokmail.net)>  
barabas.

=====

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): "[\[UNIX\] Flaws Found in Recent Linux Kernels \(newgrp, symlinks\)](#)"
  - **Messages sorted by:** [\[ date \] \[ thread \] \[ subject \] \[ author \] \[ attachment \]](#)