**TECHNICAL SERVICE BULLETIN** (TSB)

# Security Vulnerability

BRIDGE MODE AND REMOTE ADMINISTRATION USING IP ACCESS CONTROL

ComSifter®
*protect web users now!*

TSB Date: December 10, 2014

**IN THIS DOCUMENT**



## SUMMARY


A security vulnerability has been discovered in specific ComSifter models. Please review the following information for applicability to your network and potential risk.


### Models Affected

*Current models* CS-8D Pro
CS-8D

## DESCRIPTION

### Affected Scenario

The ComSifter unit must ***both*** be in Bridge Mode and have remote administration setup using IP Access Control. If the ComSifter is utilizing Static or Dynamic mode, or remote administration is not setup, then this bulletin does not apply.

> Note: If you are unsure as to which mode your ComSifter is operating in, go to `Maintenance > Information > ComSifter Information > Execute`. Under `Network Settings`, the `Connection Type` will be listed (`Bridge`, `Static`, `Dynamic/DHCP`).

### Background

The above models have a feature located in `Admin > Remote Administration` called `IP Access Control`. Within this function there is a setting called `Allow from only listed IP's`. If an IP address is entered, then the ComSifter should only allow access from the listed IP address(es). Additionally, a port forwarding rule on the upstream modem/router would have been needed to forward any request from the Internet (via port 10000) to the ComSifter.

### Issue

This function is not working as expected. Due to the nature of Bridge Mode on the ComSifter, the remote access is not coming from the listed IP address (typically a public IP address), but rather from the upstream router on the local network. The ComSifter sees the upstream router as just another IP on its subnet and allows access—regardless of the listed IP address(es) in IP Access Control. The result is that anyone on the Internet contacting the public IP address of your network (via port 10000) will get a login prompt to the ComSifter. This is a security risk as it exposes the ComSifter login prompt to the Internet. It is additionally problematic if the default username and password of the ComSifter have not been changed.

## RESOLUTION

***Immediately*** disable this function on the ComSifter—as well as remove the port forwarding from the upstream router—until further notice.

> Note: If you are affected by this bulletin, please call and have a brief discussion with our technical support group at 866-875-1254 ×702 after you have disabled this function.

Comsift, Inc. is working on a fix to the described issue and will issue an automatic software update in the near future.



**Comsift, Inc. | 1646 Elderberry Way, San Jose, CA 95125-4507 | 866-875-1254 | info@comsift.com | www.comsift.com**