

Securiteam: [NEWS] SurfControl Filter for SMTP Can Be Bypassed via Nested Zips

# [NEWS] SurfControl Filter for SMTP Can Be Bypassed via Nested Zips

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-07/0080.html>

---

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

*Date:* 07/20/03

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

Date: 20 Jul 2003 20:47:46 +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 in Canada

Toronto-based Sunrays Technologies is now Beyond Security's representative in Canada.

We welcome ISPs, system integrators and IT systems resellers

to promote the most advanced vulnerability assessment solutions today.

Contact us at 416-482-0038 or at [canadasales@beyondsecurity.com](mailto:canadasales@beyondsecurity.com)

-----  
SurfControl Filter for SMTP Can Be Bypassed via Nested Zips  
-----

## SUMMARY

SurfControl Filter for SMTP allows for SurfControl's filtering technology to be bolted on to your existing SMTP server. The rules engine contains a flaw whereby if an attachment is a .zip and it contains more than 15 zip files, the 16th zip file will not be scanned by the filter. This probably works with other archive/file types and possibly on other SurfControl products.

## DETAILS

Vulnerable systems:

\* SurfControl Filter for SMTP version 4.6

In order to bypass the filter build a .zip as below:

attach.zip – dummy\_folder – a.zip – junk.txt  
                  – b.zip – junk.txt

## Securiteam: [NEWS] SurfControl Filter for SMTP Can Be Bypassed via Nested Zips

- c.zip - junk.txt
- d.zip - junk.txt
- e.zip - junk.txt
- f.zip - junk.txt
- g.zip - junk.txt
- h.zip - junk.txt
- i.zip - junk.txt
- j.zip - junk.txt
- k.zip - junk.txt
- m.zip - junk.txt
- n.zip - junk.txt
- o.zip - junk.txt
- p.zip - junk.txt
- z.zip - sneaky.exe << Passes thru!

(The filter sorts the files in attach.zip alphabetically so we name our files a, b, c, etc to be sure that z.zip is last)

### ADDITIONAL INFORMATION

The information has been provided by <<mailto:Lee@networkpenetration.com>>  
Lee Bowyer.

=====

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.