

# [NT] McAfee WebShield SMTP Format String

---

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2006-04/msg00009.html>

---

- *From:* SecuriTeam <[support@xxxxxxxxxxxxxx](mailto:support@xxxxxxxxxxxxxx)>
  - *Date:* 5 Apr 2006 14:14:12 +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>

-----

McAfee WebShield SMTP Format String

---

## SUMMARY

"Simply plug  
<[http://www.mcafee.com/us/enterprise/products/anti\\_virus/internet\\_gateway/webshield\\_smtp.html](http://www.mcafee.com/us/enterprise/products/anti_virus/internet_gateway/webshield_smtp.html)> McAfee WebShield SMTP into virtually any network and you can scan SMTP traffic for viruses and inappropriate content, without impacting your performance-critical systems."

A format string vulnerability exists within the McAfee WebShield SMTP server which allows an attacker to execute arbitrary code on the host computer via an unauthenticated connection. With successful exploitation, an unauthenticated attacker is able to access the system.

## DETAILS

Vulnerable Systems:

- \* McAfee WebShield SMTP 4.5 MR1a

Immune Systems:

- \* McAfee Webshield SMTP 4.5 MR2

A format string vulnerability exists in the function which handles the construction of the bounce messages for non-existent domains.

[NT] McAfee WebShield SMTP Format String

On the way into the mail system this causes no problems (correct usage of the printf() family of functions). However, when the file ?(13digitfilename).rcp? is picked up from the OUT directory to construct the bounce message, a format string in the original destination address for the mail will trigger the vulnerability.

Successful exploitation can lead to remote code execution.

Vendor Status:

The vulnerability was addressed via a patch (P0803) that was released in August 2003 for Webshield SMTP 4.5 MR1a. This vulnerability has also been fixed in the latest release of the product, Webshield SMTP 4.5 MR2.

Licensed and evaluation versions of Webshield SMTP 4.5 MR2 are available for customer download from the McAfee website at <<http://www.mcafeesecurity.com/us/downloads/default.asp>>  
<http://www.mcafeesecurity.com/us/downloads/default.asp>

If there are any further questions about this statement, please contact McAfee support.  
<[http://www.mcafeesecurity.com/us/support/technical\\_support/](http://www.mcafeesecurity.com/us/support/technical_support/)>  
[http://www.mcafeesecurity.com/us/support/technical\\_support/](http://www.mcafeesecurity.com/us/support/technical_support/)

CVE Information:

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-0559>>  
CVE-2006-0559

ADDITIONAL INFORMATION

The information has been provided by  
<[mailto:CS\\_Advisories\\_Mailbox@xxxxxxxxxxxxxx](mailto:CS_Advisories_Mailbox@xxxxxxxxxxxxxx)> CS\_Advisories Mailbox .

=====

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@xxxxxxxxxxxxxx  
In order to subscribe to the mailing list, simply forward this email to: list-subscribe@xxxxxxxxxxxxxx

=====  
=====

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,

[NT] McAfee WebShield SMTP Format String

loss of business profits or special damages.