

# [UNIX] phpLinks mail() Abuse Vulnerability

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-01/0087.html>

---

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

*Date:* 01/30/03

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

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

Date: 30 Jan 2003 19:20:16 +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 would like to welcome Tiscali World Online to our service provider team.

For more info on their service offering IP-Secure, please visit [http://www.worldonline.co.za/services/work\\_ip.asp](http://www.worldonline.co.za/services/work_ip.asp)

-----

phpLinks mail() Abuse Vulnerability

---

## SUMMARY

<<http://destiney.com/2003/phplinks/>> phpLinks is a Free and Open Source PHP script. phpLinks allows you to run a very powerful link farm or search engine simulation. A vulnerability in the product allows a remote attacker to use the mail() function used by the product to send SPAM.

## DETAILS

PhpLinks has an email\_confirmation file located in the /include/ directory which is used to notify the users that they have signed up correctly. An exploit has been discovered in the file email\_confirmation.php which works as following: An attacker may call this file directly (when it should really be included) and hijack the variables in such way that he/she may abuse the mail() function. By using the example bellow, any person can use the server's SMTP service, without permission.

[target@mail.com](mailto:target@mail.com)">[http://victim.com/phplinks/include/email\\_confirmation.php?UserName=anyone&Email=target@mail.com&site\\_title=test\\_&email\\_confirmation\\_2=Hello&owner\\_name=bu&owner\\_email=I\\_Own\\_j0u@victim.com](http://victim.com/phplinks/include/email_confirmation.php?UserName=anyone&Email=target@mail.com&site_title=test_&email_confirmation_2=Hello&owner_name=bu&owner_email=I_Own_j0u@victim.com)

Side-note:

An attacker may also use this file for XSS attack on the server.

Securiteam: [UNIX] phpLinks mail() Abuse Vulnerability

Solution:

Please check the vendor's website for new patches. As a temporary solution, create a .htaccess file that contains 'Deny from all'. Place it in the /include/ directory and that should block remote users from accessing it.

ADDITIONAL INFORMATION

The information has been provided by <mailto:[mindwarper@hush.com](mailto:mindwarper@hush.com)>  
Mindwarper.

=====

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.