

# [NEWS] Multiple Buffer Overflows in Kerio Mail Server (subscribe, add\_acl, list, and do\_map)

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-06/0062.html>

---

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

*Date:* 06/19/03

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

Date: 19 Jun 2003 17:04:23 +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)

-----  
Multiple Buffer Overflows in Kerio Mail Server (subscribe, add\_acl, list, and do\_map)

---

## SUMMARY

<[http://www.kerio.com/kms\\_home.html](http://www.kerio.com/kms_home.html)> Kerio MailServer is "state-of-the-art secure email server with collaborative features suited for SME corporate environments, while providing high availability messaging for service providers". The product contains a WebMail interface that is vulnerable to buffer overflows that can lead to execution of code with system privileges.

## DETAILS

Vulnerable systems:

- \* Kerio Mail Server version 5.6.3

Multiple modules of the Kerio Mail Server (Web mail) allow remote attackers to overflow an internal buffer, causing some registers to be overwritten.

Securiteam: [NEWS] Multiple Buffer Overflows in Kerio Mail Server (subscribe, add\_acl, list, and do\_map)

http://[server]/subscribe?showuser=<More than 139><Registers>  
http://[server]/add\_acl?folder=~<More than 220  
characters><Registers>@localhost/INBOX&add\_name=lucas  
http://[Server]/list?folder=~<More than 200  
characters><Registers>@localhost/INBOX  
http://[Server]/do\_map?action=new&oldalias=eso&alias=aaa&folder=public&user=<More than 200  
characters><Registers>

ADDITIONAL INFORMATION

The information has been provided by <mailto:conde0@telefonica.net> David F.Madrid.

=====

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  
In order to subscribe to the mailing list, simply forward this email to: 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.