

# [NT] Kerio Personal Firewall Service Termination

---

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2006-07/msg00055.html>

---

- *From:* SecuriTeam <[support@xxxxxxxxxxxxxx](mailto:support@xxxxxxxxxxxxxx)>
  - *Date:* 20 Jul 2006 19:43:52 +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>

-----

## Kerio Personal Firewall Service Termination

---

### SUMMARY

Sunbelt Kerio Personal Firewall is a popular firewall software for Windows systems.

A vulnerability in the Kerio Firewall software allows to crash its service, thus bypassing the firewall.

### DETAILS

Vulnerable Systems:

- \* Sunbelt Kerio Personal Firewall 4.3.246

Immune Systems:

- \* Sunbelt Kerio Personal Firewall 4.3.268
- \* Sunbelt Kerio Personal Firewall 4.2.3.912

Kerio uses strange ring3 hooks that communicates the Kerio driver using an interrupt. Windows API CreateRemoteThread is hooked by Kerio in user mode in every process. Calling this API can cause a crash of the Kerio service 'kpf4ss.exe'. The cause of this behavior is unknown. The crash of the Kerio service equals to disabling the protection. The tray icon of Kerio

[NT] Kerio Personal Firewall Service Termination

is not functional any more after exploiting the bug, any application can perform arbitrary protected action including Internet access and process creation.

Disclosure Timeline:

- \* 2006-07-15: Vendor notification
- \* 2006-07-15: Advisory released
- \* 2006-07-17: Vulnerability confirmed by popular information sources
- \* 2006-07-17: Received request from the product vendor to temporarily remove the exploit code

ADDITIONAL INFORMATION

The information has been provided by matousec.com.  
The original article can be found at:

<http://www.matousec.com/info/advisories/Kerio-Terminating-kpf4ss-exe-using-internal-runtime-error.php>  
<http://www.matousec.com/info/advisories/Kerio-Terminating-kpf4ss-exe-using-internal-runtime-error.php>

=====

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

=====  
=====

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.