

[NT] Kaspersky Internet Security Suite klif.sys Heap Overflow Vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2007-04/msg00021.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxx>
 - *Date:* 8 Apr 2007 13:45:58 +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>

Kaspersky Internet Security Suite klif.sys Heap Overflow Vulnerability

SUMMARY

<<http://www.kaspersky.com/>> Kaspersky Internet Security Suite is "a combination of Kaspersky anti-virus, anti-spam, and personal firewall in one product". Local exploitation of a heap overflow vulnerability in Kaspersky Lab's Internet Security Suite klif.sys could allow an attacker to execute arbitrary code within kernel context.

DETAILS

Vulnerable Systems:

- * Kaspersky Internet Security version 6.0.1.411 for Windows.
- * (Previous versions may also be affected.)

The klif.sys driver is part of the "anti-hacker" proactive protection. As part of this defense, the driver hooks and screens various system calls, such as registry functions.

The hook function for the `_NtSetValueKey()` function is vulnerable to an integer overflow that leads to a kernel heap overflow. Passing a large unsigned value for the data size argument results in an arithmetic

[NT] Kaspersky Internet Security Suite klif.sys Heap Overflow Vulnerability

overflow when calculating the amount of memory to allocate. A copy operation into this buffer results in corruption of kernel memory.

Exploitation allows an attacker to execute code with kernel privileges.

This vulnerability lets an attacker overwrite a nearly arbitrary amount of kernel heap memory with arbitrary data. Exploitation of kernel heap based buffer overflows is both difficult and unreliable. However, there are documented methods for exploiting these types of overflows.

Vendor Status:

Kaspersky has addressed this vulnerability within Maintenance Pack 2. More information is available from the vendor's advisory at the following URLs.

<<http://www.kaspersky.com/technews?id=203038693>>

<http://www.kaspersky.com/technews?id=203038693>

<<http://www.kaspersky.com/technews?id=203038694>>

<http://www.kaspersky.com/technews?id=203038694>

Disclosure Timeline:

- * 01/24/2007 – Initial vendor notification
- * 03/02/2007 – Second vendor notification
- * 03/05/2007 – Initial vendor response
- * 04/03/2007 – Coordinated public disclosure

ADDITIONAL INFORMATION

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

<<http://labs.iddefense.com/intelligence/vulnerabilities/display.php?id=505>>

<http://labs.iddefense.com/intelligence/vulnerabilities/display.php?id=505>

=====

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@xxxxxxxxxxxxxxxx

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

=====
=====

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.