

[NT] Kaspersky Labs Anti-Virus IOCTL Local Privilege Escalation

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2006-10/msg00078.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxxxx>
 - *Date:* 22 Oct 2006 12:17:25 +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 Labs Anti-Virus IOCTL Local Privilege Escalation

SUMMARY

<<http://www.kaspersky.com/>> Kaspersky Anti-Virus provides virus and spyware protection.

Local exploitation of a design error vulnerability in Kaspersky Labs Anti-Virus allows an attacker to execute arbitrary code with kernel privileges.

DETAILS

Vulnerable Systems:

* Kaspersky Labs Anti-Virus version 6.0.0.303 with KCLICK and KLIN device drivers version 2.0.0.281.

The vulnerability specifically exists due to improper address space validation when the KLIN and KCLICK device drivers processes IOCTL 0x80052110. By passing a specially crafted Irp structure to the affected IOCTL handler, attackers can cause the driver to execute arbitrary code via a CALL instruction using user supplied data. Execution of data stored in user-land buffers is trivial.

[NT] Kaspersky Labs Anti-Virus IOCTL Local Privilege Escalation

Exploitation allows attackers to gain elevated privileges by executing code within kernel context. This allows attackers to gain control of the affected system. However, local access is required for exploitation to be successful.

CVE Information:

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-4926>>
CVE-2006-4926.

Disclosure Timeline:

- * 09/18/2006 – Initial vendor notification
- * 09/19/2006 – Initial vendor response
- * 10/19/2006 – 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=425>>
<http://labs.iddefense.com/intelligence/vulnerabilities/display.php?id=425>

=====

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.