

[NT] Kaspersky AntiVirus Buffer Overflow (CAB Files)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-10/0008.html>

From: SecuriTeam (*support_at_securiteam.com*)

Date: 10/06/05

To: list@securiteam.com

Date: 6 Oct 2005 15:27:54 +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 AntiVirus Buffer Overflow (CAB Files)

SUMMARY

" <<http://www.kaspersky.com/personal>> Kaspersky Anti-Virus Personal monitors all virus and spyware entry points leaving you with a clean and safe machine."

A buffer overflow vulnerability in Kaspersky AntiVirus allows attackers to cause the program execute arbitrary code using CAB archive file.

DETAILS

Vulnerable Systems:

- * Kaspersky Anti-Virus Personal version 5.0
- * Kaspersky Anti-Virus Personal Pro version 5.0
- * Kaspersky Anti-Virus version 5.0 for Windows Workstations,
- * Kaspersky Anti-Virus version 5.0 for Windows File Servers
- * Kaspersky Personal Security Suite version 1.1

Immune Systems:

- * All of Kaspersky Lab's antivirus version 4.5

Securiteam: [NT] Kaspersky AntiVirus Buffer Overflow (CAB Files)

The Kaspersky Antivirus Library provides file format support for virus analysis. During analysis of cab files Kaspersky is vulnerable to a heap overflow allowing attackers complete control of the system(s) being protected. This vulnerability can be exploited remotely without user interaction in default configurations through common protocols such as SMTP, SMB, HTTP, and FTP.

Successful exploitation of Kaspersky protected systems allows attackers unauthorized control of data and related privileges. It also provides leverage for further network compromise. Kaspersky Antivirus Library implementations are likely vulnerable in their default configuration.

The vulnerable file format engine is responsible for parsing cab files. Specifically, the vulnerability is the result of an improperly bounded copy loop in a core processing function. This function is reachable while processing records after the initial cab header. For many types of records this function is passed a statically allocated heap buffer. By crafting a cab file with large non-null records and particular header flags set, an attacker can corrupt vtables to execute arbitrary machine instructions.

A reverse engineering of a disassembler result give the following out:

```
static int CAB_read_record(CAB_FILE__struct *cfs, BYTE *dst) {
    BYTE tmp = 0;
    int count = 0;
    do {
        count++;
        cfs->CAB_fgetc(cfs, &tmp);
        if(dst) {
            *dst = tmp;
            dst++;
        }
    } while(tmp);
    ...
    Return count;
}
```

The following code copy string until a user controlled value was found, and not until destination size.

Vendor Status:

The vendor has released a patch available with regular program updates.

ADDITIONAL INFORMATION

The information has been provided by <mailto:security@rem0te.com> rem0te.

The original article can be found at:

<<http://www.rem0te.com/public/images/kaspersky.pdf>>

<http://www.rem0te.com/public/images/kaspersky.pdf>

=====

Securiteam: [NT] Kaspersky AntiVirus Buffer Overflow (CAB Files)

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.