

# [VulnWatch] iDefense Security Advisory 03.02.07: Kaspersky AntiVirus UPX File Decompression DoS Vulnerability

---

*Source:* <http://www.derkeiler.com/Mailing-Lists/VulnWatch/2007-03/msg00000.html>

---

- *From:* iDefense Labs <[labs-no-reply@xxxxxxxxxxxx](mailto:labs-no-reply@xxxxxxxxxxxx)>
  - *Date:* Fri, 02 Mar 2007 13:35:21 -0500
- 

Kaspersky AntiVirus UPX File Decompression DoS Vulnerability

iDefense Security Advisory 03.02.07  
<http://labs.iddefense.com/intelligence/vulnerabilities/>  
Mar 02, 2007

## I. BACKGROUND

Kaspersky Antivirus is a popular client and gateway virus scanner for Unix and Windows. UPX, the ultimate packer for executables, is a method for compressing executable files to reduce their size on disk. For more information, visit the vendor's site at the following URL.

<http://www.kaspersky.com/>

## II. DESCRIPTION

Remote exploitation of a denial of service (DoS) vulnerability in Kaspersky Lab's Antivirus could allow an attacker to conduct a DoS attack on a targeted host.

The antivirus engine is vulnerable to a DoS condition when processing an executable packed with UPX compression. Malformed compressed data causes the decompression routine to enter an infinite loop. Specifically, a negative data offset results in the same compressed data chunk being processed endlessly.

## III. ANALYSIS

Exploitation allows an attacker to conduct a DoS attack.

If this attack is conducted against an e-mail gateway running Kaspersky, legitimate clients may be unable to send e-mail through the server.

The infinite loop being executed consists of a short sequence of instructions, which results in maximum CPU usage. On a client desktop, the

infinite loop will render the machine nearly unusable. On a server, it severely degrades the quality of service of other applications running.

#### IV. DETECTION

iDefense has confirmed the existence of this vulnerability in Kaspersky Labs Antivirus Engine version 6.0.1.411 for Windows and 5.5–10 for Linux. Previous versions may also be affected. Any products that use the scanning engine are also affected, which includes the Kaspersky e-mail gateway scanner.

#### V. WORKAROUND

iDefense is currently unaware of any workarounds for this issue.

#### VI. VENDOR RESPONSE

Kaspersky Lab reports that it has fixed this vulnerability as of February 7th, 2007. In addition, they stated the following.

"There is no need to download any special patches. All installed Kaspersky Lab products are updated automatically through the regular signature-update functionality. There is not need to contact Kaspersky Lab to obtain this fix."

#### VII. CVE INFORMATION

A Mitre Corp. Common Vulnerabilities and Exposures (CVE) number has not been assigned yet.

#### VIII. DISCLOSURE TIMELINE

01/24/2007 Initial vendor notification  
03/01/2007 Initial vendor response  
03/02/2007 Coordinated public disclosure

#### IX. CREDIT

The discoverer of this vulnerability wishes to remain anonymous.

Get paid for vulnerability research  
<http://labs.idefense.com/methodology/vulnerability/vcp.php>

Free tools, research and upcoming events  
<http://labs.idefense.com/>

#### X. LEGAL NOTICES

Copyright © 2007 iDefense, Inc.

Permission is granted for the redistribution of this alert electronically.

It may not be edited in any way without the express written consent of iDefense. If you wish to reprint the whole or any part of this alert in any other medium other than electronically, please e-mail customerservice@xxxxxxxxxxxx for permission.

Disclaimer: The information in the advisory is believed to be accurate at the time of publishing based on currently available information. Use of the information constitutes acceptance for use in an AS IS condition. There are no warranties with regard to this information. Neither the author nor the publisher accepts any liability for any direct, indirect, or consequential loss or damage arising from use of, or reliance on, this information.