

[VulnWatch] iDefense Security Advisory 01.05.07: Kaspersky Antivirus Scan Engine PE File Denial of Service Vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/VulnWatch/2007-01/msg00005.html>

- *From:* iDefense Labs <labs-no-reply@xxxxxxxxxxxxx>
 - *Date:* Fri, 05 Jan 2007 17:13:16 -0500
-

Kaspersky Antivirus Scan Engine PE File Denial of Service Vulnerability

iDefense Security Advisory 01.05.07
<http://labs.iddefense.com/intelligence/vulnerabilities/>
Jan 05, 2007

I. BACKGROUND

Kaspersky Antivirus is a popular client and gateway virus scanner. For more information see their site:

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

II. DESCRIPTION

Remote exploitation of a DoS vulnerability in Kaspersky Lab's Antivirus could allow an attacker to cause a denial of service (DoS) condition.

Kaspersky Antivirus is vulnerable to a DoS condition when processing a specially crafted PE (portable executable) file. One of the headers in a PE file is the Optional Windows Header section. This section of the PE header contains information needed by the Windows linker and loader. An invalid value for the 'NumberOfRvaAndSizes' field will cause Kaspersky to repeatedly seek and read from the same section of the file in an endless loop.

III. ANALYSIS

Exploitation allows attackers to send the scanning engine into an infinite loop. Further attempts to scan files will be prevented.

Exploitation requires that an attacker sends a specially constructed PE file through an e-mail gateway or personal anti-virus client using the Kaspersky scanning engine.

IV. DETECTION

iDefense has confirmed the existence of this vulnerability in Kaspersky Labs Antivirus Engine version 6.0 for Windows and 5.5–10 for Linux. Previous versions may also be affected. Any products that use the scanning engine are also affected. This includes the Kaspersky mail gateway scanner.

V. WORKAROUND

iDefense is currently unaware of any effective workarounds for this issue.

VI. VENDOR RESPONSE

Kaspersky Lab reports that it has fixed this vulnerability as of January 2nd, 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

12/12/2006 Initial vendor notification
12/12/2006 Initial vendor response
01/05/2007 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 © 2006 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@xxxxxxxxxxxxx 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.