

# [VulnWatch] iDefense Security Advisory 12.08.06: Multiple Vendor Antivirus RAR File Denial of Service Vulnerability

---

*Source:* <http://www.derkeiler.com/Mailing-Lists/VulnWatch/2006-12/msg00010.html>

---

- *From:* iDefense Labs <[labs-no-reply@xxxxxxxxxxxxx](mailto:labs-no-reply@xxxxxxxxxxxxx)>
  - *Date:* Fri, 08 Dec 2006 17:56:23 -0500
- 

Multiple Vendor Antivirus RAR File Denial of Service Vulnerability

iDefense Security Advisory 12.08.06  
<http://labs.iddefense.com/intelligence/vulnerabilities/>  
Dec 08, 2006

## I. BACKGROUND

AntiVirus products typically handle searching files for known viruses within their scan engines. Most scan engines support searching inside of known archive types for viruses as well. For more information refer to any of the popular AntiVirus vendors' web sites.

## II. DESCRIPTION

Remote exploitation of a denial of service vulnerability in Multiple Vendors' Antivirus engines allows an attacker to cause the engines to consume excessive resources.

The affected vendors' scan engines are vulnerable to a DoS attack when scanning specially malformed RAR archives. Specifically, the malformed archives will have the `head_size` and `pack_size` fields set to zero in Archive Header section. When such a file is encountered, the affected scan engines will enter an infinite loop.

## III. ANALYSIS

Successful exploitation will allow an attacker to cause the affected scan engine to consume excessive CPU, and in some cases memory, resources. The malicious RAR file would need to be uploaded to a server to initiate the attack. Several common ways this could be achieved are e-mail attachments, available network shares, FTP accounts, or Web form uploads.

The impact of the vulnerability varies slightly from vendor to vendor as described below.

#### Sophos:

Scanning of archives is not enabled by default and must be specified by the user. This denial of service attack will prevent the scanner from scanning other files on disk while it is stuck on the exploit file. The hung process can be stopped by the user.

#### Trend Micro:

Once attacked, the scan engine will consume 99 percent of CPU resources and the affected computer will require a reboot to recover from the condition. The scan engine process cannot be forced to quit, although its thread priority can be lowered to regain some use of the system before reboot.

### IV. DETECTION

iDefense has confirmed this vulnerability exists in the following vendors' products. This should not be considered an exhaustive list as these vendors tend to include the scan engine in many of their products. Previous versions are likely to be affected as well.

- \* Sophos Small business edition (Windows/Linux) 4.06.1 with engine version 2.34.3.
- \* Trend Micro PC Cillin – Internet Security 2006
- \* Trend Micro Office Scan 7.3
- \* Trend Micro Server Protect 5.58

### V. WORKAROUND

For Sophos' scan engine, this exploit will not have any effect if the "Enabled scanning of archives" option is not set. iDefense is currently unaware of a workaround for this issue for the remaining vendor's engines.

### VI. VENDOR RESPONSE

Sophos has addressed this problem with new versions of their products. See <http://www.sophos.com/support/knowledgebase/article/7609.html> for more information.

Trend Micro stated that this vulnerability does not affect version 8.320 of their Windows scan engine. Additionally, they have released version 8.150 of the HPUX and AIX builds of their scan engine to address this problem in those environments.

### VII. CVE INFORMATION

The Common Vulnerabilities and Exposures (CVE) project has assigned the name CVE-2006-5645 to this issue. This is a candidate for inclusion in the CVE list (<http://cve.mitre.org>), which standardizes names for security problems.

### VIII. DISCLOSURE TIMELINE

09/27/2006 Initial vendor notifications  
09/27/2006 Initial vendor response – Trend Micro  
09/28/2006 Initial vendor response – Sophos  
12/08/2006 Coordinated public disclosure

## IX. CREDIT

The vulnerability was reported by Titon of BastardLabs, Damian Put <pucik@xxxxxxxxxxx>, and an anonymous researcher.

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

Free tools, research and upcoming events  
<http://labs.odefense.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 email customerservice@xxxxxxxxxxx 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.