

# [VulnWatch] iDefense Security Advisory 10.15.06: Clam AntiVirus ClamAV rebuildpe Heap Overflow Vulnerability

---

*Source:* <http://www.derkeiler.com/Mailing-Lists/VulnWatch/2006-10/msg00015.html>

---

- *From:* iDefense Labs <[labs-no-reply@xxxxxxxxxxxxx](mailto:labs-no-reply@xxxxxxxxxxxxx)>
  - *Date:* Mon, 16 Oct 2006 16:03:57 -0400
- 

Clam AntiVirus ClamAV rebuildpe Heap Overflow Vulnerability

iDefense Security Advisory 10.15.06

<http://www.idefense.com/intelligence/vulnerabilities/>

Oct 15, 2006

## I. BACKGROUND

Clam AntiVirus is a multi-platform GPL anti-virus toolkit. The main purpose of which is integration into electronic mail servers. More information is available from <http://clamav.net/>

## II. DESCRIPTION

Remote exploitation of a buffer overflow in Clam AntiVirus allows attackers to potentially execute arbitrary code or cause a denial of service condition.

This vulnerability specifically exists within code dealing PE (Portable Executable) format files. While processing certain PE elements, two variables can be very large and integer overflow could occur. This would result in less memory being allocated than was expected by the programmer and subsequent code would overflow the heap buffer.

## III. ANALYSIS

Successful exploitation requires an attacker to send a specially constructed executable file through a mail gateway or personal anti-virus client utilizing the ClamAV scanning engine.

## IV. DETECTION

iDefense has confirmed this vulnerability on version 0.88.1 and 0.88.4 of ClamAV. All previous versions are suspected to be vulnerable to this issue.

## V. WORKAROUND

iDefense is not aware of any effective workarounds.

## VI. VENDOR RESPONSE

The ClamAV team has addressed this vulnerability within version 0.88.5.

## VII. CVE INFORMATION

The Common Vulnerabilities and Exposures (CVE) project has assigned the name CVE-2006-4182 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

08/16/2006 Initial vendor notification  
08/20/2006 Initial vendor response  
10/10/2006 Second vendor notification  
10/15/2006 Coordinated public disclosure

## IX. CREDIT

The discovery of this vulnerability is credited to Damian Put  
<pucik@xxxxxxxxxxxx>.

Get paid for vulnerability research  
<http://www.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 email 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.