

# [Full-disclosure] AVG Anti-Virus – Arbitrary Code Execution (remote)

---

*Source:* <http://www.derkeiler.com/Mailing-Lists/Full-Disclosure/2006-11/msg00205.html>

---

- *From:* <[security@xxxxxxxx](mailto:security@xxxxxxxx)>
  - *Date:* Mon, 13 Nov 2006 16:24:23 +0100
- 

n.runs AG  
<http://www.nruns.com/> security at nruns.com  
n.runs-SA-2006.002 13-Nov-2006

---

Vendor: Grisoft Inc., <http://grisoft.com>  
Product: AVG Anti-Virus  
Vulnerability: Arbitrary Code Execution (remote)

---

## Vendor communication:

2006/08/24 initial notification to Grisoft Inc.  
2006/08/24 Grisoft Inc. Response  
2006/08/25 PGP keys exchange  
2006/08/25 PoC files sent to Grisoft Inc.  
2006/08/30 Bugs Confirmation, Timeframe Coordination for patches  
development and testing  
2006/09/20 Grisoft Inc. released Update with fixes

---

## Overview:

Grisoft is focused on developing software solutions that provide protection from computer viruses. Grisoft's primary focus is to deliver the most comprehensive and proactive protection available on the market.

Distributed globally through resellers and through the internet, the AVG Anti-Virus product line supports all major operating systems and platforms. More than 40 million users around the world use Grisoft AVG products to protect their computers and networks.

## Description:

Multiple vulnerabilities have been found in the file parsing engine.

[Full-disclosure] AVG Anti-Virus – Arbitrary Code Execution (remote)

In detail, the following flaws were determined:

- Heap Overflow through Integer Overflow in .CAB file parsing
- Uninitialized Variable flaw in .CAB file parsing.
- Divide by Zero in .DOC file parsing.
- Heap Overflow through Integer Overflow in .RAR file parsing
- Integer Issues in .EXE file parsing.

These problems can lead to remote arbitrary code execution if an attacker carefully crafts a file that exploits one or more of the aforementioned vulnerabilities. The vulnerabilities are present in AVG Antivirus software versions prior to 7.1.407.

Solution:

The vulnerabilities were reported on Aug 24 and the fixes were released on Sep 20. The updated software versions are available from <http://www.grisoft.com/doc/10/lng/us/tpl/tpl01>

---

Credit:

Bugs found by Sergio Alvarez of n.runs AG. Thanks.

Thanks.

---

References: <http://www.grisoft.com/doc/36365/lng/us/tpl/tpl01>

---

The information provided is released by n.runs "as is" without warranty of any kind. n.runs disclaims all warranties, either express or implied, except for the warranties of merchantability. In no event shall n.runs be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages, even if n.runs has been advised of the possibility of such damages.

Distribution or Reproduction of the information is provided that the advisory is not modified in any way.

Copyright 2006 n.runs. All rights reserved. Terms of use.

---

Full-Disclosure – We believe in it.

Charter: <http://lists.grok.org.uk/full-disclosure-charter.html>

Hosted and sponsored by Secunia – <http://secunia.com/>