

n.runs AG  
<http://www.nruns.com/>  
n.runs-SA-2007.010

[security\(at\)nruns.com](mailto:security(at)nruns.com)  
28-May-2007

---

Vendor: Avira GmbH, <http://www.avira.com>  
Affected Product: Avira Antivir Antivirus  
Vulnerability: Arbitrary Code Execution (remote)  
Risk: HIGH

---

Vendor communication:

2007/05/07	initial notification to Avira GmbH
2007/05/07	Avira GmbH Response
2007/05/08	PGP public keys exchange
2007/05/09	PoC files sent to Avira GmbH
2007/05/10	Avira GmbH acknowledged and validated the PoC files
2007/05/16	Avira GmbH sent fix release schedule and fixed engine
2007/05/17	Sergio Alvarez tested fixed engine
2007/05/23	Avira GmbH released Update with fixes

---

Overview:

Avira, a company with over 15 millions customers and more than 250 employees is a worldwide leading supplier of self-developed security solutions for professional and private use. With more than 20 years of experience, the company is one of the pioneers in this field.

In addition to programs specifically for use on single workstations, Avira primarily offers professional solutions for cross-system protection of networks on various levels. These include products for workstations, file, mail and web servers. Gateway computers can be managed as workstation computers via a central management console for all operating systems. In addition to the management products of the individual solutions, security programs for PDAs, smartphones and embedded devices are also offered.

Avira AntiVir Personal, used by millions of private users, represents a significant contribution to security.

Description:

A remotely exploitable vulnerability has been found in the file parsing engine.

In detail, the following flaw was determined:

- Buffer Overflow through Integer Cast Around in .LZH file parsing

Impact:

This problem can lead to remote arbitrary code execution if an attacker carefully crafts a file that exploits the aforementioned vulnerability. The vulnerability is present in Avira Antivir Antivirus software versions prior to the update Version 7.03.00.09.

Solution:

The vulnerability was reported on 07.May.2007 and an update has been issued on 23.May.2007 to solve this vulnerability through the regular update mechanism.

---

Credit:

Bugs found by Sergio Alvarez of n.runs AG.

---

References:

<http://forum.antivir-pe.de/thread.php?threadid=22528>

This Advisory and Upcoming Advisories:

[http://www.nruns.com/security\\_advisory.php](http://www.nruns.com/security_advisory.php)

---

Unaltered electronic reproduction of this advisory is permitted. For all other reproduction or publication, in printing or otherwise, contact [security@nruns.com](mailto:security@nruns.com) for permission. Use of the advisory constitutes acceptance for use in an "as is" condition. All warranties are excluded. 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.

Copyright 2007 n.runs AG. All rights reserved. Terms of apply.