

n.runs AG
<http://www.nruns.com/>
n.runs-SA-2007.009

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

Vendor: ALWIL Software a.s., <http://www.avast.com>
Affected Product: avast! antivirus
Vulnerability: Arbitrary Code Execution (remote)
Risk: HIGH

Vendor communication:

2007/05/07	initial notification to ALWIL Software a.s.
2007/05/07	ALWIL Software a.s. Response
2007/05/07	PoC files sent to ALWIL Software a.s.
2007/05/09	ALWIL Software a.s. Response
2007/05/09	resent PoC files sent to ALWIL Software a.s.
2007/05/09	ALWIL Software a.s. acknowledge the PoC files
2007/05/10	ALWIL Software a.s. issued the fix for testing
2007/05/16	ALWIL Software a.s. released Update with fixes

Overview:

The company specializes in security software, with avast! antivirus being the flagship product line. During the lifetime of the product line, avast! products have become both award winning, and number one in a number of key markets, as well as increasing market share year-on-year since first international release.

On 11th May 2007 avast@! antivirus Home Edition reached 30 million registered users.

Description:

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

In detail, the following flaw was determined:

- Heap Overflow through Integer Cast Around in .SIS 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 avast! Antivirus software versions prior to the update Version 4.7.700.

Solution:

The vulnerability was reported on 07.May.2007 and an update has been issued on 16.May.2007 to solve this vulnerability through the regular update mechanism.

Credit:

Bugs found by Sergio Alvarez of n.runs AG.

References:

<http://www.avast.com/eng/adnm-management-client-revision-history.html>

<http://www.avast.com/eng/search.php?searchFor=sergio+alvarez>

This Advisory and Upcoming Advisories:

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 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.