
Vendor: Panda Software, <http://www.pandasoftware.com>
Affected Products: Panda Antivirus
Vulnerability: Arbitrary Code Execution (remote)
Risk: HIGH

Vendor communication:

2007/05/07	Initial notification to Panda Software
2007/05/08	Panda Software Response and pgp keys exchange
2007/05/09	PoC files sent to Panda Software
2007/05/10	Panda Software has some problems to reproduce it
2007/05/10	Assess to Panda Software to reproduce the bug
2007/05/24	Panda Software works on the vulnerability
2007/05/25	Panda Software first beta fix
2007/06/01	Ping to Panda Software for update on fix status
2007/06/03	Panda Software fix in QA
2007/07/05	Ping to Panda Software for status update
2007/07/05	Panda Software fix still in QA
2007/07/13	Panda Software notify tentative release date
2007/07/20	Panda Software made available the updates

Overview:

Founded in 1990 in Bilbao, Spain, Panda Software is privately owned and has been self-financed from the start. With a strong focus on innovation and research, it became a market leader in Spain in 1995 and started its international expansion in 1996. In 2007, Investindustrial and Gala Capital entered Panda Software's share capital as part of a strategy to undertake an aggressive expansion plan and globally launch new IT security solution.

Today the company maintains its international headquarters in Bilbao and Madrid, and counts on a network of 3 subsidiaries (USA, Spain, France), a joint-venture in China and 56 exclusive franchises in as many countries around the world. The company sells its products and services to consumers and businesses in over 200 countries around the world.

Panda Software is a leading developer and provider of integrated security solutions to combat viruses, hackers, Trojans, spyware, phishing, spam and other Internet threats.

Panda Software's centrally managed security solutions protect servers, gateways and endpoints, ensuring an effective and simple-to-use line of defense against Internet threats for enterprises, small and medium-sized businesses and home users.

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 .EXE 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 Panda Antivirus software versions prior to the last update of 20.Jul.2007.

Solution:

The vulnerability was reported on May 07 and an update has been issued on July 20 to solve this vulnerability through the regular update mechanism.

Credit:

Bugs found by Sergio Alvarez of n.runs AG.

References:

Vendor Acknowledgement:

"Panda Software would like to thank Sergio 'shadown' Alvarez of nruns.com for reporting this issue and working responsibly with us to release a fix in order to protect users."

This Advisory and Upcoming Advisories:

http://www.nruns.com/security_advisory.php

<http://www.nruns.com/parsing-engines-advisories.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.