

Vendor: Sophos, <http://www.sophos.com>
Affected Products: Sophos Anti-Virus for Windows
Sophos Anti-Virus for Unix/Linux
Vulnerability: Arbitrary Code Execution (remote)
Risk: HIGH

Vendor communication:

2007/05/07	initial notification to Sophos
2007/05/09	Sophos Response
2007/05/14	PGP public keys exchange
2007/05/14	PoC files sent to Sophos
2007/05/17	Sophos acknowledged the PoC files
2007/05/17	Sophos Corporation validate the Vulnerability
2007/05/17	Sophos notify tentative update release date
2007/07/31	Sophos notify a delay in the update release date
2007/08/23	Sophos Update with fixes released
2007/08/29	Sophos contacts n.runs AG to discuss Exploitability
2007/09/03	Sophos updates the advisory

Overview:

Sophos is a world leader in IT security and control solutions purpose-built for business, education, government organizations and service providers. Their reliably engineered, easy-to-operate products protect over 100 million users in more than 150 countries from viruses, spyware, adware, Trojans, intrusion, spam, policy abuse, and uncontrolled network access.

Description:

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

In detail, the following flaw was determined:

- One BYTE Overwrite in Arbitrary Location caused by an Integer Handling issue while parsing the UPX format.

Impact:

This problem can lead to remote denial of service or arbitrary code execution if an attacker carefully crafts a file that exploits the aforementioned vulnerability. The vulnerability is present in Sophos Anti-virus software listed above on all platforms supported by the affected products prior to the engine Version 2.48.0.

Solution:

The vulnerability was reported on 07.May.2007 and an update has been issued on 23.Aug.2007 to solve this vulnerability. For detailed information about the fixes follow the link in the References [1]

section of this document.

n.runs AG wants to highlight the excellent and fluent communication with Sophos.

Credit:

Bugs found by Sergio Alvarez of n.runs AG.

References:

<http://www.sophos.com/support/knowledgebase/article/28407.html> [1]

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 use apply.