

# [NEWS] Symantec AntiVirus Library Heap Overflow

**Source:** <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-02/0035.html>

---

**From:** SecuriTeam (*support\_at\_securiteam.com*)

**Date:** 02/13/05

To: list@securiteam.com

Date: 13 Feb 2005 11:04:41 +0200

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>

-- promotion

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.

<http://www.securiteam.com/maillinglist.html>

-----

Symantec AntiVirus Library Heap Overflow

---

## SUMMARY

X-Force has discovered a vulnerability in Symantec AntiVirus Library. The Symantec AntiVirus Library is widely relied upon to provide AntiVirus capabilities to desktop, server, and gateway systems. Also, several large vendors and ISP's implement Symantec's AntiVirus Library in their products. By crafting a UPX file, an attacker is able to trigger a heap overflow within the process importing the Symantec AntiVirus Library.

## DETAILS

Vulnerable Systems:

- \* Symantec Norton Antivirus 2004 for Windows
- Symantec Norton Internet Security 2004 (pro) for Windows
- Symantec Norton System Works 2004 for Windows
- Symantec Norton Antivirus 2004 for Macintosh
- Symantec Norton Internet Security 2004 for Macintosh
- Symantec Norton System Works 2004 for Macintosh
- Symantec Norton Antivirus 9.0 for Macintosh
- Symantec Norton Internet Security for Macintosh 3.0
- Symantec Norton System Works for Macintosh 3.0
- Norton AntiVirus for Microsoft Exchange 2.1 prior to build 2.18.85
- Symantec Mail Security for Microsoft Exchange 4.0 prior to build

## Securiteam: [NEWS] Symantec AntiVirus Library Heap Overflow

4.0.10.465

Symantec Mail Security for Microsoft Exchange 4.5 prior to build 4.5.3

Symantec AntiVirus/Filtering for Domino NT 3.1 prior to build 3.1.1

Symantec Mail Security for Domino 4.0 prior to build 4.0.1

Symantec AntiVirus/Filtering for Domino Ports 3.0

(AIX) prior to build 3.0.6

(OS400, Linux, Solaris) prior to build 3.0.7

Symantec AntiVirus Scan Engine 4.3 prior to build 4.3.3

Symantec AntiVirus for Network Attached Storage prior to build 4.3.3

Symantec AntiVirus for Caching prior to build 4.3.3

Symantec AntiVirus for SMTP 3.1 prior to build 3.1.7

Symantec Mail Security for SMTP 4.0 prior to build 4.0.2

Symantec Web Security 3.0 prior to build 3.0.1.70

Symantec BrightMail AntiSpam 4.0

Symantec BrightMail AntiSpam 5.5

Symantec AntiVirus Corporate Edition 9.0 prior to build 9.01.1000

Symantec AntiVirus Corporate Edition 8.01, 8.1.1

Symantec Client Security 2.0 prior to build 9.01.1000

Symantec Client Security 1.0, 1.0

Symantec Gateway Security 2.0, 2.0.1 5400 Series

Symantec Gateway Security 1.0 5300 Series

Note: Additional versions may be affected, please contact your vendor for confirmation. In addition, several ISPs and vendors also use Symantec AntiVirus Library and are likely vulnerable.

Compromise of antivirus protected networks and machines may lead to exposure of confidential information, loss of productivity, and further network compromise. Successful exploitation of this vulnerability could be used to gain unauthorized access to networks and machines being protected by Symantec AntiVirus Library product. Implementations of Symantec AntiVirus Library are likely vulnerable through common protocols, e.g. SMTP, HTTP, FTP. No authentication is required for an attacker to leverage this vulnerability to compromise an antivirus protected network or machine. It is likely Symantec AntiVirus Library implementations are vulnerable in their default configurations.

Symantec Antivirus Library is used to parse different file formats to detect malware. One of the modules (DEC2EXE) in Symantec Antivirus Library parses the UPX (Ultimate Packer for eXecutables) file format. Before UPX decompression, the library does not properly check a virtual file offset when reconstructing the Portable Executable (PE) header. An attacker may provide a negative virtual offset to a crafted PE header, which contains integers used for bounds calculations on subsequent copy operations to buffers allocated on integers from the legitimate PE header. The result is an arbitrary heap overflow with no character restrictions.

This vulnerability can be triggered by an unauthenticated remote attacker, without user interaction, by sending an e-mail containing a crafted UPX file to the target Symantec AntiVirus Library on client, server, and gateway implementations. Additional attack vectors exist over other common protocols (e.g. HTTP, FTP, POP3), but some may require user interaction.

Securiteam: [NEWS] Symantec AntiVirus Library Heap Overflow

Additional Information:

Symantec has issued an advisory. For more details see:

<<http://www.symantec.com/avcenter/security/Content/2005.02.08.html>>

<http://www.symantec.com/avcenter/security/Content/2005.02.08.html>

ADDITIONAL INFORMATION

The information has been provided by X-Force.

The original article can be found at:

<<http://xforce.iss.net/xforce/alerts/id/187>>

<http://xforce.iss.net/xforce/alerts/id/187>

=====

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:

[list-unsubscribe@securiteam.com](mailto:list-unsubscribe@securiteam.com)

In order to subscribe to the mailing list, simply forward this email to: [list-subscribe@securiteam.com](mailto:list-subscribe@securiteam.com)

=====

=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.