

[NEWS] Symantec Antivirus RAR Library Multiple Heap Overflows

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-12/msg00099.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxx>
 - *Date:* 28 Dec 2005 12:02:21 +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 RAR Library Multiple Heap Overflows

SUMMARY

The <<http://www.symantec.com/>> Symantec Antivirus library "provides file format support for virus analysis". During decompression of RAR files the Symantec Antivirus library can be caused to overflow multiple heap allocations, this would allow attackers to cause the program using this library to execute arbitrary code.

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

[NEWS] Symantec Antivirus RAR Library Multiple Heap Overflows

- * Symantec Mail Security for Microsoft Exchange 4.0 prior to build 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 and 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

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.

CVE Information:

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0249>>
CAN-2005-0249

ADDITIONAL INFORMATION

The information has been provided by <<mailto:list@xxxxxxxxxx>> rem0te.com.

The original article can be found at:

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

[NEWS] Symantec Antivirus RAR Library Multiple Heap Overflows

The vendor advisory can be found at:

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

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

The vendor Knowledge Base can be found at:

<<http://service1.symantec.com/SUPPORT/ent-security.nsf/docid/2005020911112648>>

<http://service1.symantec.com/SUPPORT/ent-security.nsf/docid/2005020911112648>

=====

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@xxxxxxxxxxxxxxx

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@xxxxxxxxxxxxxxx

=====

=====

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.

-
- Prev by Date: [*\[UNIX\] Kpdf/Koffice Multiple Buffer Overflows \(Xpdf\)*](#)
 - Next by Date: [*\[UNIX\] Sudo Perl Local Privileges Escalation*](#)
 - Previous by thread: [*\[UNIX\] Kpdf/Koffice Multiple Buffer Overflows \(Xpdf\)*](#)
 - Next by thread: [*\[UNIX\] Sudo Perl Local Privileges Escalation*](#)
 - Index(es):
 - ◆ [*Date*](#)
 - ◆ [*Thread*](#)