

[NT] McAfee VirusScan DUNZIP32.dll Buffer Overflow

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2006-04/msg00000.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxxxx>
 - *Date:* 2 Apr 2006 13:44:44 +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>

McAfee VirusScan DUNZIP32.dll Buffer Overflow

SUMMARY

" <<http://us.mcafee.com/root/package.asp?pkgid=100&cid=16269>> VirusScan – Always–updated protection against PC viruses. Safeguard your hard drive, email, attachments and downloads from known and unknown viruses, mass–mailing worms, Trojans and potentially unwanted programs (PUPs) like spyware."

McAfee ViruScan anti–virus software is confirmed as affected to a remote buffer overflow vulnerability in a 3rd–party compression library.

DETAILS

Vulnerable Systems:

* DynaZip library versions 5.00.03 and prior.

The vulnerability is caused due to a boundary error in a 3rd–party compression library's (DUNZIP32.dll) old, vulnerable version used when handling packed signature files. InnerMedia DynaZip compression library mentioned is responsible for virus description file unpacking operations. This can be exploited to cause a buffer overflow via a specially crafted

[NT] McAfee VirusScan DUNZIP32.dll Buffer Overflow

signature file. When a specially crafted virus definition package containing a file with an overly long filename (a file name or files inside a package) is opened the attacker may be able to execute arbitrary code on user's system (see VU#582498 reference). Opening of signature file is an automatic operation of product's SecurityCenter.

The following file was copied to C:\Program Files\McAfee.com\Shared directory during an installation process when tested:

File name: dunzip32.dll

Time stamp: 8th April, 2005

File version: 3.0.0.14

Description: DynaZIP-32 Multi-Threading UnZIP DLL

Copyright information: Copyright (c) Inner Media, Inc. 1993-1996, All Rights Reserved.

The following processes use Dunzip32.dll library:

C:\PROGRA~1\McAfee.com\Agent\mcupdmgr.exe (McAfee SecurityCenter Update Manager v6.x)

C:\PROGRA~1\McAfee.com\Shared\mghtml.exe (McAfee Security HTML Dialog v4.x)

From US-CERT <<http://www.kb.cert.org/vuls/id/582498>> VU#582498:

"Impact: If a remote attacker can persuade a user to access a specially crafted zip file, the attacker may be able to execute arbitrary code on that user's system possibly with elevated privileges."

Solution:

Vendor has issued a patch shipped with immune library version 5.00.06. It can be obtained by downloading an updated product version or using product's SecurityCenter Updates feature.

Non-affected library has the following time stamp: 30th December, 2005.

According to vendor response localized builds has been fixed as well.

Tested non-affected product version: Build 10.0.27

Vendor is reportedly in process to publish FAQ (version release) document to the McAfee/Network Associates KnowledgeBase

(
<http://knowledgemap.nai.com/KanisaSupportSite/supportcentral/supportcentral.do?id=m1&language=en_US>
http://knowledgemap.nai.com/KanisaSupportSite/supportcentral/supportcentral.do?id=m1&language=en_US).

Workaround:

No working workarounds available.

CVE Information:

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2004-1094>>
CVE-2004-1094

US-CERT:

<<http://www.kb.cert.org/vuls/id/582498>> VU#582498

[NT] McAfee VirusScan DUNZIP32.dll Buffer Overflow

Disclosure Timeline:

- * 23-Dec-2005 – Vulnerability researched and confirmed
- * 29-Dec-2005 – Vendor was contacted
- * 30-Dec-2005 – Vendor's reply
- * 11-Jan-2006 – AVERT Labs informs about started version testing process
- * 02-Mar-2006 – New contact to the vendor
- * 02-Mar-2006 – Vendor's reply, issue was fixed on 24th January, vendor informs about upcoming FAQ release document
- * 27-Mar-2006 – New contact to the vendor asking the state of FAQ release
- * 30-Mar-2006 – Security companies and several CERT units contacted
- * 30-Mar-2006 – Public disclosure

ADDITIONAL INFORMATION

The information has been provided by <<mailto:juha-matti.laurio@xxxxxxxx>>
Juha-Matti Laurio.

The original article can be found at:

<<http://www.networksecurity.fi/advisories/mcafee-virusscan.html>>
<http://www.networksecurity.fi/advisories/mcafee-virusscan.html>

=====

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@xxxxxxxxxxxxxxxx

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

=====

=====

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.