

[NT] Vulnerability in Virtual PC and Virtual Server Allows Elevation of Privilege (MS07-049)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2007-08/msg00022.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxxxx>
 - *Date:* 19 Aug 2007 08:59:03 +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>

Vulnerability in Virtual PC and Virtual Server Allows Elevation of Privilege (MS07-049)

SUMMARY

An elevation of privilege vulnerability exists in Microsoft Virtual PC and Microsoft Virtual Server that could allow a user with administrator permissions to the guest operating system to run code on the host operating system or other guest operating systems. An attacker with administrator permissions to the guest operating system, could exploit the vulnerability by running specially crafted code on the guest operating system. This could result in a heap overflow on the host or other guest operating systems. An attacker who successfully exploited this vulnerability could take complete control of an affected system.

DETAILS

Affected and Non-Affected Software

The software listed here has been tested to determine which versions or editions are affected. Other versions or editions are either past their support life cycle or are not affected. To determine the support life cycle for your software version or edition, visit Microsoft Support Lifecycle.

[NT] Vulnerability in Virtual PC and Virtual Server Allows Elevation of Privilege (MS07-049)

Affected Software

Affected Software – Maximum Security Impact – Aggregate Severity Rating –

Bulletins Replaced by This Update

*

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=E2C72AAB-00DE-47C9-8ECB-09261C4B7DEB>>

Microsoft Virtual PC 2004 – Elevation of Privilege – Important – None

*

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=2BDA2B8B-9C1C-4BF8-9A65-491092276E7A>>

Microsoft Virtual PC 2004 Service Pack 1 – Elevation of Privilege – Important – None

*

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=F9EC76CD-0607-4394-BC49-35E95D02DA51>>

Microsoft Virtual Server 2005 Standard Edition – Elevation of Privilege – Important – None

*

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=A35E556C-2F7B-4B72-9662-AE7286573C3F>>

Microsoft Virtual Server 2005 Enterprise Edition – Elevation of Privilege – Important – None

*

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=D44B8669-A4FB-4CBA-B130-E1BC08B10C6F>>

Microsoft Virtual Server 2005 R2 Standard Edition – Elevation of Privilege – Important – None

*

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=84CA3BA9-6575-4C5B-8F8E-4E4A635A4705>>

Microsoft Virtual Server 2005 R2 Enterprise Edition – Elevation of Privilege – Important – None

* <<http://www.microsoft.com/mac/downloads.aspx#VPC>> Microsoft Virtual PC
for Mac Version 6.1 – Elevation of Privilege – Important – None

* <<http://www.microsoft.com/mac/downloads.aspx#VPC>> Microsoft Virtual PC
for Mac Version 7 – Elevation of Privilege – Important – None

Non-Affected Software

* Microsoft Virtual PC 2007

* Microsoft Virtual Server 2005 R2 Service Pack 1

CVE Information:

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0948>>

CVE-2007-0948

ADDITIONAL INFORMATION

The information has been provided by <<mailto:security@xxxxxxxxxxxxx>>
Microsoft Product Security.

The original article can be found at:

<<http://www.microsoft.com/technet/security/bulletin/ms07-049.msp>>

<http://www.microsoft.com/technet/security/bulletin/ms07-049.msp>

=====

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@xxxxxxxxxxxxxxxxx

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

=====

=====

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.