

[NEWS] VMWare Workstation Guest Isolation Vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2007-02/msg00010.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxxx>
 - *Date:* 5 Feb 2007 17:42:16 +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>

VMWare Workstation Guest Isolation Vulnerability

SUMMARY

<<http://www.vmware.com/>> VMware Workstation "software consists of a virtual machine suite for Intel x86-compatible computers. This software suite allows users to set up multiple x86 virtual computers and to use one or more of these virtual machines simultaneously with the hosting operating system". Issues in the way VMWare handles the guest operating system allows malicious programs installed under VMWare to access sensitive information stored under the clipboard.

DETAILS

Vulnerable Systems:

- * VMware Workstation, version 5.5.3 build 34685 (including installation of "VMware tools" of the same version on the guest OS).
- * (Other products by the vendor using the same isolation components may be effected as well, but they weren't tested due to lack of resources. I advise administrators who use the corporate products of VMware to test this issues if they use this products in a production environment)

Guest and Host OS:

[NEWS] VMWare Workstation Guest Isolation Vulnerability

- * Windows XP Pro with SP2 and all the latest operational and security patches from the "windows update" site, up to 31-Jan-2007.
- * (Other guest OS (especially ones by Microsoft) maybe effected as well, but they weren't tested).

Each VM has its own settings. one settings category is "Guest Isolation", which includes a checkbox named "Enable copy and paste to and from this virtual machine". This feature can work only if the "VMware tools" component is installed on the guest OS. The clipboard copy operation can transfer only text, not files or streams. Eitan has discovered the following issues regarding this component:

1. Changing the value of this feature (in either way enabling or disabling) becomes actually active only if a global operation is made towards the guest OS, like suspend and resume, reset, restart (from within the guest OS), shutdown (either from within the guest OS or by performing a "power off" from the VMware workstation application) and then turning it back on. Simply changing the check box value and pressing OK will not change current functionality of this feature.
2. When this feature is turned on and working The direction of the clipboard content transfer is the same as the direction of the focus change between guest and host operating systems and vice versa. But, when the host OS clipboard is empty and the focus is moved to the guest OS clipboard the guest clipboard is not cleared and left with its current content. Now, when focusing back to the host's, empty, source clipboard it is now filled with the content of the guest's clipboard thus the host clipboard is failing to keep itself erased and its previously cleared content is re-filled from the guest OS. This behavior may re-fill the host's clipboard with data that was intentionally erased (like password or credit card number). Strangely, this behavior does not happen when the process is started from the guest OS clipboard, and if it is the first to be erased, and then the focus moves to the host, the host's clipboard is erased. So, the issue here is only when the process starts from the host side.

Possible Abuses:

1. Issue 1 – The VMware administrator might turn on the clipboard transfer and use it, but when he will turn it off by un-checking the check box it will remain active thus transferring text objects (a password, for example), from one clipboard to another, in any direction while the administrator will believe the environments are separated and isolated. This brakes the promised isolation, and may cause information leakage and may infect any OS (host or guest) if the text is a string that can be run as a command or URL when it will unintentionally be pasted into a command line interface and activated.
2. Issue 2 – The VMware user will clear his host clipboard (from a copied password, for example) and think it is cleared. But the content that was cleared may have been previously copied to the guest clipboard and when the focus will move back to the host the content will re-enter the host's

[NEWS] VMWare Workstation Guest Isolation Vulnerability

clipboard. (General note: To my opinion VMware has, regarding the isolation features, a significant lack of security measures like setting permissions for specific users and groups, at the host and at the guest, (or simply a password) to allow or prohibit performing data transfer (clipboard and/or drag & drop) and the allowed data transfer directions).

Reproduction:

(You might wish to use the freeware clipclear (<http://www.moonsoftware.com/freeware.asp>) for a visual sign of when the clipboard is full or empty and for clearing the clipboard)

Issue 1:

1. When the test VM is turned off (one with the "VMware tools" pre-installed), make sure the "Enable copy and paste to and from this virtual machine" checkbox is checked (VM settings -> "Options" tab -> "Guest Isolation" line -> "Enable copy and paste to and from this virtual machine").
2. Turn on the VM and log into the guest OS.
3. Copy any text in the guest OS.
4. Move the focus to the host and paste the clipboard into any text field verify the text is the same as the one copied in the guest OS.
5. Copy a different text in the host OS.
6. Move the focus back to the guest OS and paste the clipboard to any text field - verify the text is the same as the one copied from the host OS.
7. Turn off the "Enable copy and paste to and from this virtual machine" from the VM settings and click OK.
8. Repeat steps 3 to 6 and verify you are able to perform them, although the relevant option is now "disabled".
9. You can repeat steps 1 to 8 but this time in the other way round, by starting with the check box as un-checked.
10. Activate the change by performing one of the following operations towards the guest OS: either suspend and resume, reset (from the VMware hosting application), restart (from within the guest OS), shutdown (either from within the guest OS or by performing a "power off" from the VMware hosting application) and then turning it back on. After performing either operation make sure the change was applied.

Issue 2:

1. When the test VM is turned off (one with the "VMware tools" pre-installed), make sure the "Enable copy and paste to and from this virtual machine" checkbox is checked (VM settings -> "Options" tab -> "Guest Isolation" line -> "Enable copy and paste to and from this virtual machine").
2. Turn on the VM and log into the guest OS.
3. Move the focus to the host OS and copy the word "password".
4. Move the focus to the guest OS and paste the clipboard into any text field.
5. Make sure the word "password" is displayed.
6. Move back to the host OS and clear the clipboard content. Make sure it is clear by pasting its content to a text field and verify nothing was

[NEWS] VMWare Workstation Guest Isolation Vulnerability

pasted.

7. Move the focus to the guest OS and then back to the host OS and again perform a paste action to a text field.

9. Verify that now the clipboard has pasted the word "password".

Direct resolution:

Not any that Eitan is aware of at the time of writing this advisory.

Workarounds:

Issue 1: No workaround was found.

Issue 2: Disabling the clipboard transfer on a global level, for all of the VMs immediately – by clearing the following checkbox in VMware workstation interface:

"Edit" menu -> "Preferences" command -> "Input" tab -> "Enable copy and paste to and from virtual machine". If this global option is turned off, than at each VM level, clipboard copy, in any direction, will not be allowed, regardless of the current actual clipboard copy status at each VM. Remember that this option effects ALL of the virtual machines used within the VMware workstation.

Vendor Status:

The vendor was notified at the end of September 2006, but it could not commit to any planned date for a fix regarding both issues.

ADDITIONAL INFORMATION

The information has been provided by <<mailto:eitancaspi@xxxxxxxxxx>> Eitan Caspi.

=====

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.