

[NT] Flaw in Microsoft VM JDBC Classes Could Allow Code Execution

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-09/0079.html>

From: support@securiteam.com

Date: 09/22/02

From: support@securiteam.com

To: list@securiteam.com

Date: Sun, 22 Sep 2002 20:51:08 +0200 (CEST)

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

When was the last time you checked your server's security?

How about a monthly report?

<http://www.AutomatedScanning.com> -- Know that you're safe.

Flaw in Microsoft VM JDBC Classes Could Allow Code Execution

SUMMARY

The Microsoft VM is a virtual machine for the Win32 operating environment. The Microsoft VM shipped in most versions of Windows (a complete list is available in the FAQ), as well as in most versions of Internet Explorer. It also was available for some time as a separate download. A new patch for the Microsoft VM is available, which eliminates three security vulnerabilities. The attack vectors for all of them would likely be the same. An attacker would likely create a web page that, when opened, exploits the desired vulnerability, and either host it on a web page or send it to a user as an HTML mail.

The first vulnerability involves the Java Database Connectivity (JDBC) classes, which provide features that allow Java applications to connect to and use data from a wide variety of data sources, ranging from flat files to SQL Server databases. The vulnerability results because of a flaw in the way the classes vet a request to load and execute a DLL on the user's system. Although the classes do perform checks that are designed to ensure that only authorized applets can levy such a request, it is possible to spoof this check by constructing a malformed request in a particular way, thereby enabling an attacker to load and execute any DLL on the user's system.

Securiteam: [NT] Flaw in Microsoft VM JDBC Classes Could Allow Code Execution

The second vulnerability also involves the JDBC classes, and occurs because certain functions in the classes do not correctly validate handles that are provided as input. One straightforward use of this flaw would involve supplying invalid data in lieu of an actual handle when calling such a function. Microsoft has confirmed that this scenario would cause Internet Explorer to fail. In addition, there is at least a theoretical possibility that the flaw also could enable an attacker to provide data that would have the effect of running code in the security context of the user.

The third vulnerability involves a class that provides support for the use of XML by Java applications. This class exposes a number of methods; some of these are suitable for use by any applet, while others are only suitable for use by trusted ones. However, the class does not differentiate correctly between these cases, and instead makes all of the methods available to all applets. Among the functions that could be misused through this vulnerability are ones that would enable an applet to take virtually any desired action on the user's system.

DETAILS

Affected Software:

* Versions of the Microsoft virtual machine (Microsoft VM) are identified by build numbers, which can be determined using the JVIEW tool as discussed in the FAQ. All builds of the Microsoft VM up to and including build 5.0.3805 are affected by these vulnerabilities.

Mitigating factors:

* In order to exploit any of these vulnerabilities via the web-based attack vector, the attacker would need to entice a user into visiting a web site that the attacker controlled. The vulnerabilities themselves provide no way to force a user to a web site.

* Java applets are disabled within the Restricted Sites Zone. As a result, any mail client that opened HTML mail within the Restricted Sites Zone, such as Outlook 2002, Outlook Express 6, or Outlook 98 or 2000 when used in conjunction with the Outlook Email Security Update, would not be at risk from the mail-based attack vector.

* The vulnerability would gain only the privileges of the user, so customers who operate with less than administrative privileges would be at less risk from the vulnerability.

* Corporate IT administrators could limit the risk posed to their users by using application filters at the firewall to inspect and block mobile code.

Patch availability:

Download locations for this patch

* Download location for this patch:

<<http://windowsupdate.microsoft.com/>> Windows Update

Securiteam: [NT] Flaw in Microsoft VM JDBC Classes Could Allow Code Execution

What new vulnerabilities are eliminated by this patch?

There are three vulnerabilities addressed by this patch:

- * A vulnerability that could make it possible for an attacker to gain control over another user's system via a flaw in a database support function.

- * A vulnerability that, at the least, could enable an attacker to cause Internet Explorer to fail.

- * A vulnerability that could make it possible for an attacker to gain control over another user's system via a flaw in a function that supports XML.

Users who have disabled Java applets using the Internet Explorer security settings cannot be affected by any of these vulnerabilities.

What is the Microsoft VM?

The Microsoft virtual machine (Microsoft VM) implements the Java programming language on Windows platforms. The Microsoft VM is included in most versions of Windows, is included in most versions of Internet Explorer, and was available for some time as a separate download. The vulnerabilities here affect all customers who have the Microsoft VM.

I do not know if the Microsoft VM is installed on my system. How can I tell?

If you are using any of the following versions of Windows, you definitely have the Microsoft VM installed:

- * Microsoft Windows 95
- * Microsoft Windows 98 and 98SE
- * Microsoft Windows Millennium
- * Microsoft Windows NT 4.0, beginning with Service Pack 1
- * Microsoft Windows 2000
- * Microsoft Windows XP, beginning with Service Pack 1

The Microsoft VM also shipped as part of several versions of Internet Explorer and other products, so even customers using Windows NT 4.0 Gold or Windows XP Gold could potentially have it installed. If you are in doubt about whether you have it installed, do the following:

- 1) Select Start, then Run.
- 2) Type "cmd" (without the quotes), then hit the enter key
- 3) In the resulting command box, type "Jview" (without the quotes). If a program runs, you have the Microsoft VM installed. If you receive an error saying that no program by that name exists, you do not.

Is this a new version of the Microsoft VM?

No. Although in many previous cases we have delivered security fixes by releasing new versions of the Microsoft VM (also known as builds), in this case we have released a patch that should be applied to the current version, build 3805.

Securiteam: [NT] Flaw in Microsoft VM JDBC Classes Could Allow Code Execution

How can I tell what version of the Microsoft VM I am using?

Here is how to determine the build number you are using:

- 1) Select Start, and then Run.
- 2) On Windows 95, 98, or Me, type "command" (without the quotes). On Windows NT 4.0, 2000, or XP, type "cmd" (again, without the quotes). Hit the enter key.
- 3) In the result command box, type "Jview" (without the quotes) and hit the enter key.
- 4) In the topmost line of the resulting listing, you should see a version number of the form x.yy.zzzz. The final four digits are the version number.

Once I know the version number, what should I do?

Use the table below to determine the right action.

If the version number is. . .

Less than 3805

You should. . .

Upgrade to build 3805, then apply the patch. (Both are available from Windows Update).

If the version number is. . .

3805

You should. . .

Apply the patch. (Available from Windows Update).

If the version number is. . .

More than 3805

You should. . .

Do nothing. You are using a version that is already protected against these vulnerabilities.

I am a network administrator. I see that the patch is available on Windows Update, but I would like to download it and install it on my users' systems. Can I do this?

1. Go to the Windows Update web site.
2. In the left pane, under Other Options, select "Personalize Windows Update".
3. Under "Set Options for Windows Update", select the checkbox for "Display the Link to Windows Update Catalog under 'See Also'", and then click "Save Settings".
4. Go back to the Windows Update web site.
5. In the left pane, under "See Also", select "Windows Update Catalog".
6. Select "Find Updates for Microsoft Operating Systems".
7. Select the operating system and language of your choice.
8. Select "Critical Updates and Service Packs".
9. Select all of the patches you would like to download, then click on "Go to download basket" to download them.

Securiteam: [NT] Flaw in Microsoft VM JDBC Classes Could Allow Code Execution

DLL execution via JDBC classes:

What is the scope of this vulnerability?

This vulnerability could enable an attacker to gain complete control over a user's system. This would enable the attacker to perform any operation that the user could, such as running applications; communicating with web sites; adding, deleting, or changing data; and other actions.

The vulnerability could only be exploited if a user visited a web site hosted by an attacker, or opened an HTML mail that had been sent by the attacker. However, the latter scenario would be ineffective if the user were using Outlook 2002, Outlook Express 6, or was using either Outlook 98 or 2000 in conjunction with the Outlook Email Security Update.

What causes the vulnerability?

The vulnerability results because the JDBC classes do not adequately police requests to load DLLs. Although they do check such requests and attempt to block any that originate from untrusted applets, these checks can be bypassed.

What are the JDBC classes?

The Java Database Classes (JDBC) is a set of functions that are provided to allow Java programs to use databases. For instance, they provide functions that allow programs to open and use the data within text files, SQL Server databases, and a variety of other types of databases.

What is wrong with the JDBC classes?

Among the functions provided by the JDBC classes is one that enables a Java program to load and execute a dynamic link library (DLL) on the user's system. Because DLLs are programs and, once running, have all the privileges of the user himself, only a trusted program should be able to load and execute one.

The JDBC classes do check all requests to load and run DLLs and, by design, should turn away requests that do not come from trusted programs. However, a flaw exists in the way these checks are done, and it is possible to malformed a request in such a way that the JDBC will comply with the request even though it came from an untrusted program.

What would this vulnerability enable an attacker to do?

An attacker who successfully exploited this vulnerability would be able to load and execute any desired DLL on the user's system. The specific effect of exploiting the vulnerability would depend on the particular DLL the attacker executed, but even the DLLs that install as part of Windows include functions that could be misused to cause significant damage. It is likely that in most cases additional DLLs would be available to the attacker (for instance, those that were installed as part of an application), and these could allow even greater damage, potentially giving the attacker complete control over the user's system.

How might someone exploit this vulnerability?

The attacker would need to create a web page that calls the appropriate

Securiteam: [NT] Flaw in Microsoft VM JDBC Classes Could Allow Code Execution

JDBC function in the way described above. When the page was opened, it would attempt to exploit the vulnerability. The web page could be hosted on a web site as a means of attacking any visitors to the site, or the attacker could mail the page directly to users as an HTML mail in order to exploit vulnerability against people who received and opened it.

You said the web page could "attempt" to exploit the vulnerability. What would determine whether this attempt was successful?

The critical factor would be whether Java was enabled on the user's system. The Internet Explorer Security Zones mechanism provides a way of regulating what actions various web sites can take – among them, whether they can run Java applets. By default, web pages in the Restricted Sites Zone cannot run Java applets. This turns out to be especially significant in the case of an attack via the HTML mail vector.

Why is that?

By default, Outlook Express 6.0 and Outlook 2002 open HTML mails in the Restricted Sites Zone. In addition, Outlook 98 and 2000 open HTML mails in the Restricted Sites Zone if the Outlook Email Security Update has been installed. Customers who use any of these products would be at no risk from the email attack vector.

How does the patch address this vulnerability?

The patch adds additional checks to eliminate the spoofing vulnerability.

Handle Validation Flaw:

What is the scope of this vulnerability?

Microsoft has confirmed that, through this vulnerability, an attacker could cause Internet Explorer to fail. However, there is a possibility, as yet unconfirmed, that it could also enable an attacker to gain control over a user's system. The avenues for exploiting the vulnerability, as well as the protective measure available to users, are the same as those discussed above.

What causes the vulnerability?

The vulnerability results because at least one function in the JDBC classes does not adequately validate handle data that has been provided as input.

What are handles?

Handles are a type of data that, as the name suggests, facilitate the handling and use of things – in this case, data structures, files, and other operating system objects. When a function needs to manipulate an object that is owned by the caller, it is typical for the function to accept a handle to the object as one of the input parameters.

What is wrong with the way the Microsoft VM works with handles?

Some of the functions in the JDBC classes accept handles as input parameters, but do not adequately validate the data they receive before using it. Instead, these functions blindly use whatever the caller provides them.

Securiteam: [NT] Flaw in Microsoft VM JDBC Classes Could Allow Code Execution

What would the effect of using invalid handle data be?

It would depend on the specific data. In every case that Microsoft is aware of, the effect of supplying invalid handle data would be to cause the hosting application – Internet Explorer – to fail. However, there is a theoretical, although yet undemonstrated, possibility that cases exist through which invalid handle data could be used to enable the caller to cause Internet Explorer to take action of the attacker's choice.

How might someone exploit this vulnerability?

The attack vectors for this vulnerability are the same as those discussed above. An attacker would need to either host a web site and entice users into visiting it, or send it directly to selected users as HTML mail.

Would the preventative measures discussed above work equally well against this vulnerability?

Yes. As discussed above, the web-based attack vector could be blocked via the Internet Explorer security settings, and the web-based vector could be blocked by most recent Microsoft mail clients.

How does the patch address the vulnerability?

The patch institutes proper validation of inputs in the functions that have the flaw.

Inappropriate methods exposed in XML support classes:

What is the scope of this vulnerability?

This vulnerability has the same scope as the vulnerability discussed above, both in terms of the effect of the vulnerability, the means by which it could be exploited, and the preventative steps a user could take.

What causes the vulnerability?

A Java class that is provided to support the use of XML via Java exposes a set of methods to all programs, when in fact they are only appropriate for trusted programs to use.

What is XML?

XML (Extensible Markup Language) can be thought of as a universal data format that allows web applications written in different programming language to exchange data with each other. The Microsoft VM provides a class of functions that facilitate the use of XML by Java programs. The vulnerability lies in those functions.

What is wrong with the XML support class?

The XML support class makes a number of different functions available for use by Java programs. By design, some of these should be available to all Java programs, and others should only be available to trusted programs. Instead, all of the functions are available to all Java programs.

What kind of functions are you talking about?

Among the functions in this class are ones that allow programs to manipulate the contents of system memory. Clearly, such functions should only be exposed to trusted programs, because any program that could

Securiteam: [NT] Flaw in Microsoft VM JDBC Classes Could Allow Code Execution

manipulate system memory could, for instance, alter programs already in memory and make them perform new functions.

What would this vulnerability enable an attacker to do?

An attacker who successfully exploited the vulnerability could take any desired action on the user's system. The only limiting factor would be the user's privileges on the system. That is, if the user had administrative privileges on the system, the attacker's program could gain administrative privileges as well; on the other hand, if the user had only limited privileges on the system, the attacker's program would have only limited privileges as well.

How might someone exploit this vulnerability?

The attack vectors for this vulnerability are the same as those discussed above. An attacker would need to either host a web site and entice users into visiting it, or send it directly to selected users as HTML mail.

Would the preventative measures discussed above work equally well against this vulnerability?

Yes. As discussed above, the web-based attack vector could be blocked via the Internet Explorer security settings, and the web-based vector could be blocked by most recent Microsoft mail clients.

How does the patch address the vulnerability?

The patch institutes checks to ensure that programs can only use the functions that are appropriate for the degree to which they are trusted.

ADDITIONAL INFORMATION

The information has been provided by

<mailto:0_36906_E51E4D7D-DECD-43AE-9A29-36080E8D4C3C_US@Newsletters.Microsoft.com>
Microsoft Product Security.

=====

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

In order to subscribe to the mailing list, simply forward this email to: 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.

-
- **Previous message:** support@securiteam.com: "[NEWS] The Trivial Cisco IP Phones Compromise"
 - **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)