

# [NT] Vulnerabilities in Microsoft's Java implementation

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-09/0049.html>

---

*From:* [support@securiteam.com](mailto:support@securiteam.com)

*Date:* 09/12/02

From: [support@securiteam.com](mailto:support@securiteam.com)

To: [list@securiteam.com](mailto:list@securiteam.com)

Date: Thu, 12 Sep 2002 13:27:34 +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.

-----

Vulnerabilities in Microsoft's Java implementation

---

## SUMMARY

Microsoft Internet Explorer comes with Java virtual machine and accompanying class packages. Multiple security vulnerabilities have been found in the Java environment. Some of these allow an attacker to deliver and run arbitrary code on the Internet Explorer or Outlook user's system when a hostile web site or mail message is viewed.

The latest versions of the software are affected by the flaws, but Outlook (Express) users are not vulnerable to the mail-based attack if the security zone of mail is set to Restricted. This is the default case with Outlook Express 6 and Outlook with the latest security updates. In this case, Java Applets are not shown at all in mail messages; if Applets are shown, then the user is vulnerable.

## DETAILS

Background:

Java Applets are small Java programs that can be embedded inside HTML documents. Applets are generally secure because the Java environment enforces strict security policies for them. Applets are enabled by default in most web browsers today.

## Securiteam: [NT] Vulnerabilities in Microsoft's Java implementation

As opposed to normal executable programs, Java Applets do not contain machine language code but special "bytecode" which is interpreted by the Java virtual machine, a kind of simulated processor. Bytecode does not have direct means of controlling the processor or operating system's resources.

Java applications in general can do file or network operations just like any program. Applets are treated differently; because Applets contain untrusted code supplied by web sites (or anyone sending you mail), they are run within a strictly bound "sandbox". They cannot access local files and their allowed network operations are very limited. When the Java environment is implemented correctly, untrusted Applets can't do anything dangerous. The flaws discussed here are not related to the Java or Applet concepts, but individual implementations of them.

### Details:

There were more than ten (10) different Java vulnerabilities found and reported to Microsoft. Some of these allow file access on the viewer's system, some allow access to other resources, and some allow delivery and execution of arbitrary program code on the victim system. These attacks can be carried out when a web page or mail message containing a hostile Applet is viewed with Internet Explorer or Outlook. In this case, the Applet may upload any program code and start it. The code can do any operations the user can do – read or modify files, install or remove programs, etc.

The vulnerabilities are mostly related to native methods and their improper or missing parameter checking. There are also some logical mistakes and some problems in package, field, or method visibility (i.e. public/protected/private). Some of the vulnerabilities deal with system independent memory address, which makes exploiting them more difficult; some of the more serious ones do not require such information.

Native methods are pieces of ordinary machine language code contained by Java classes. Technically their code comes from DLL's, but within Java, they look like ordinary Java methods.

An Applet cannot contain native methods for obvious reasons, but many of the core Java classes contain them. For instance, all file operations are eventually done by native methods. They are used to do operations that are not possible or practical to do in pure Java. They may be also used for speed-critical parts of the code. Native methods are not bound by the Java security policies and can access the processor, operating system, memory, and file system.

Security-wise, native methods are a weak link. Unlike ordinary Java code, they can contain traditional programming flaws like buffer overflows. If an untrusted Java Applet can invoke a native method containing a security flaw, it may be able to escape its sandbox and compromise the system.

## Securiteam: [NT] Vulnerabilities in Microsoft's Java implementation

In most Java implementations, there are many native methods scattered in the core Java classes. Many of them are declared private so that an Applet cannot directly invoke them. In some of these cases, a hostile Applet may still call another method that in turn may pass some of the parameters to a private native method. If the parameters are not checked adequately by the Java code passing them, an Applet might be able to do unwanted operations even if the native method does not have flaws.

Most of these vulnerabilities do not seem to originate from the original Sun Microsystems's code, but the modifications or additions made by Microsoft. Sun's Java Plug-in was tested against them but no knowingly exploitable vulnerabilities seem to exist.

Any detailed technical information has been left out of this advisory in order to prevent exploitation of the vulnerabilities. Due to the educational value, it may be published later.

### Workarounds:

Microsoft was first contacted in July 2002 and started their investigation of potential Java vulnerabilities. More of them were found during August and reported to the vendor. Microsoft has acknowledged most of the vulnerabilities and is currently working on a patch to correct them.

To protect themselves, Internet Explorer and Outlook (Express) users can disable Java Applets until the patch is released. This can be done in Internet Options -> Security -> Internet -> Custom Level -> Microsoft VM, select "Disable Java".

If you want to use an Applet on a certain web site you trust, you can add the site to the Trusted Sites zone and enable Applets in that zone.

### ADDITIONAL INFORMATION

The information has been provided by <<mailto:jouko@solutions.fi>> Jouko Pynnonen.

=====

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](mailto:list-unsubscribe@securiteam.com)

In order to subscribe to the mailing list, simply forward this email to: [list-subscribe@securiteam.com](mailto: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.

Securiteam: [NT] Vulnerabilities in Microsoft's Java implementation

- *Previous message:* [support@securiteam.com](mailto:support@securiteam.com): "[UNIX] phpGB Cross Site Scripting Bug"
- *Messages sorted by:* [\[ date \]](#) [\[ thread \]](#) [\[ subject \]](#) [\[ author \]](#) [\[ attachment \]](#)