

[NT] Console Java Applications can Leak Passphrases on Windows

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-06/0064.html>

From: support@securiteam.com

Date: 06/17/02

From: support@securiteam.com

To: list@securiteam.com

Date: Mon, 17 Jun 2002 20:56:39 +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.

Console Java Applications can Leak Passphrases on Windows

SUMMARY

In certain circumstances, Java[TM] applications using the standard nCipher ConsoleCallBack class on Windows NT/2000 can be made to leak smart card passphrases to the current user's shell.

One version of the nCipher command line utility 'TrustedCodeTool', as supplied to CodeSafe customers, is also affected by this problem.

DETAILS

Background:

1. Smart cards and passphrases

The master secrets for a Security World are protected by the Administrator Card Set; application keys can be protected either by the master secrets (module protection), or by further smart cards known as Operator Card Sets.

Each card can be further protected by a passphrase, which must be provided before the secret share on the card can be read. In such cases, the authorization becomes two-factor: 'something you have' plus 'something you know'.

2. kmjava and the ConsoleCallBack

nCipher's suite of development kits under the CipherTools and CodeSafe brand names include Java support. In particular, the `kmjava` component provides a Java interface to the Security World, and is further used by the nCipher JCE CSP and CodeSafe/J.

Java programs using the Security World are required to provide a callback object which is responsible for interacting with the user during operations which require the loading of a set of smart cards. Kmjava includes the class `com.ncipher.km.nfkm.ConsoleCallBack` which performs such interactions, and example code demonstrating its use.

Issue details:

1. Cause

One of the functions performed by the ConsoleCallBack is the reading of a passphrase from the user, when the user wishes to load a smart card which is protected by a passphrase.

The mechanism employed to read this passphrase turns out to be incompatible with version 1.4.0 of the Java Runtime Environment on Windows platforms. A passphrase prompt appears as expected, but the calling program does not resume after the user has entered their passphrase. If the user subsequently assumes the application has hung and presses Control-C in an attempt to kill it, their command shell receives the user's passphrase as if they had typed it there.

2. Impact

A site running Java software on Windows which makes use of the ConsoleCallBack will find it ceases to work and potentially leaks passphrases, in the manner described above, if they upgrade from a previous version of the Java 2 Platform to v1.4.0.

If the user's command shell supports history tracking, the history file will also contain the entered passphrase if it has been leaked in the manner described.

Note that this issue only affects the host the ConsoleCallBack is running on, and not the HSM. The security of the HSM is unaffected. However, an attacker who is able to gain control of sufficient smart cards having observed their passphrases could gain unauthorized access to application keys, especially if the smart cards in question form an Administrator Card Set.

3. Who May Be Affected

This problem affects users:

- * That are using nForce or nShield modules, and
- * Running software which makes use of the ConsoleCallBack, and
- * Running under version 1.4.0 of the Java Runtime Environment on the Windows operating system, and
- * Only in circumstances where this software requires to read passphrases from the console in order to load a cardset.

Securiteam: [NT] Console Java Applications can Leak Passphrases on Windows

This includes users of the Java version of nCipher's 'TrustedCodeTool', as supplied to many CodeSafe customers and end-users.

This problem does not affect KeySafe, or the original Trusted Code Tool (trustedcodetool.exe, as supplied to some early CodeSafe customers) or its latest revision (tct2.exe, currently under limited release).

4. How To Tell If You Are Affected

It is usually possible to determine the installed version(s) of the Java Runtime Environment by consulting the 'Add/Remove Programs' Control Panel. At the time of writing, the only known affected versions are '1.4.0' and '1.4.0_01'; earlier versions are *not* affected.

Be aware that it is possible to install multiple versions of the JRE on a system, and that certain applications may make use of different installed versions. If you are in any doubt as to which versions of the JRE are used by an application, please contact your application vendor.

To determine if you have kmjava installed, examine your system for the presence of 'c:\nfast\lib\versions\kmjava-atv.txt' (or 'lib\versions\kmjava-atv.txt' within the install directory if you have installed the nCipher software to a non-default location). If this file is present, so is kmjava; otherwise, you are not affected.

If the smart cards to be read by the application are not protected by passphrases, you are not affected.

5. Vendor-specific notes

nCipher

The java version of the 'TrustedCodeTool', as supplied to many CodeSafe customers and end-users, is affected by this issue. If you have an early version of CodeSafe which included 'trustedcodetool.exe', or a very recent version which contains 'tct2.exe', you are *not* affected.

A software update is in development and will be made available via nCipher Support in due course.

Others

To determine whether a third-party application makes use of the ConsoleCallBack, please contact the application vendor. (As a general rule, if an application never requires loading the smart cards, or is completely GUI-based, it is unlikely to be affected. Certain applications do not support the use of passphrases on smart cards, and are similarly not affected.)

Remedy:

1. Users who are NOT running an affected version of the JRE
We advise users to not upgrade their installation of the Java Runtime Environment to version 1.4.0 until revised versions of kmjava and supporting components are available, or if advised by their application vendor(s) that it is safe to do so.

Securiteam: [NT] Console Java Applications can Leak Passphrases on Windows

2. Users who ARE running an affected version of the JRE

We advise users who are running a potentially affected application on an affected version of the JRE to revert to an earlier version of the JRE if their application supports it.

If the application and site security policy allow, it may be reasonable to remove passphrase protection from the smart cards to be loaded. Otherwise, please contact the application vendor for advice.

3. CodeSafe users

We advise users of the nCipher Java 'TrustedCodeTool' not to operate it with JRE version 1.4.0 if the cardset(s) to be loaded are protected by passphrases. (It remains supported under JRE versions 1.2.x and 1.3.x.)

It is safe to use the TCT if the smart cards to be loaded are not passphrase protected, or if the passphrase protection is removed (provided your site security policy allows this).

A software update is in development and will be made available via nCipher Support in due course.

4. Users who have inadvertently leaked smart card passphrases

We recommend users change any leaked passphrase(s) at once. Please refer to the section entitled 'Changing a pass phrase' in the nForce or nShield User Guide, and any documentation to this effect provided by your application vendor, if applicable.

We further advise users to determine how many passphrases have been leaked and consider whether this may have compromised the security of their keys and the impact this may have on their security assumptions.

ADDITIONAL INFORMATION

The information has been provided by <mailto:support@ncipher.com> nCipher Support.

=====

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.

Securiteam: [NT] Console Java Applications can Leak Passphrases on Windows

- *Previous message:* support@securiteam.com: "[NT] Resin DOS device Denial of Service"
- *Messages sorted by:* [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)